ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Algebra 276 (2004) 340–370

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Finite imprimitive linear groups of prime degree

J.D. Dixon [a,*] and A.E. Zalesski [b]

[a] *School of Mathematics and Statistics, Carleton University, Ottawa ON K2G 0E2, Canada*
[b] *School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK*

Received 6 May 2003

Communicated by Jan Saxl

Abstract

In an earlier paper the authors classified the nonsolvable primitive linear groups of prime degree over $\mathbb{C}$. The present paper deals with the classification of the nonsolvable imprimitive linear groups of prime degree (equivalently, the irreducible monomial groups of prime degree). If G is a monomial group of prime degree r, then there is a projection π of G onto a transitive group H of permutation matrices with a kernel A consisting of diagonal matrices. The transitive permutation groups of prime degree are known, so the classification reduces to (i) determining the possible diagonal groups A for a given group H of permutation matrices; (ii) describing the possible extensions which might occur for given A and H; and (iii) determining when two of these extensions are conjugate in the general linear group. We prove that for given nonsolvable H there is a finite set $\Phi(r, H)$ of diagonal groups such that all monomial groups G with $\pi(G) = H$ can be determined in a simple way from the monomial groups which are extensions of $A \in \Phi(r, H)$ by H, and calculate $\Phi(r, H)$ in many cases. We also show how the problem of determining conjugacy in the general case is reduced to solving this problem when $A \in \Phi(r, H)$. In general, the results hold over any algebraically closed field with modifications required in the case of a few small characteristics.

1. Introduction

This paper is concerned with the problem of describing the finite imprimitive linear groups of prime degree over an algebraically closed field. It complements earlier work [7,20] describing the primitive linear groups of prime degree over $\mathbb{C}$. Since the degree is prime, the classification of imprimitive groups is equivalent to classification of irreducible

* Corresponding author.
E-mail addresses: jdixon@math.carleton.ca (J.D. Dixon), a.zalesskii@uea.ac.uk (A.E. Zalesski).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2004.02.005

monomial groups (see below). Considerable work has been done on classifying the solvable monomial groups of prime degree; see [5,19,28,29], and related work [1,10,18, 25]. Therefore in this paper we restrict ourselves to nonsolvable, imprimitive groups of prime degree.

We now establish notation which will be used throughout the rest of the paper. In all cases r will denote a prime and F will be an algebraically closed field. Suppose that G is a finite nonsolvable imprimitive subgroup of $GL(V)$ where V is a vector space of dimension r over F. Because r is prime, the definition of imprimitivity shows that there exists a basis $e_1, \ldots, e_r$ of V such that G permutes the set of 1-dimensional subspaces $Fe_1, \ldots, Fe_r$ transitively. Over this basis the elements of G correspond to matrices from the monomial group $\mathrm{Mon}(r, F)$. We shall identify G with this group of monomial matrices and V with the vector space F^r of r-vectors over F, so $e_1, \ldots, e_r$ is just the standard basis of F^r. The elements of $GL(r, F)$ which permute the set $\{Fe_1, \ldots, Fe_r\}$ of 1-dimensional subspaces are just the elements of $\mathrm{Mon}(r, F)$, whilst the elements which fix each of the subspaces Fe_i form the *diagonal group* D. The elements of $GL(r, F)$ which map the set $\Omega := \{e_1, \ldots, e_r\}$ into itself form the group S of *permutation matrices* in $\mathrm{Mon}(r, F)$. Note that S is isomorphic to the symmetric group $\mathrm{Sym}(r)$, D is abelian, and $\mathrm{Mon}(r, F) = DS$. Finally, we define Z to be the group of scalar matrices, so Z is the centre of $GL(r, F)$.

We shall consider a further simplification. For each subgroup K of $GL(r, F)$ we define $K^0 := K \cap SL(r, F)$. In particular, Z^0 has order r when $\mathrm{char}(F) \neq r$ (otherwise it is 1). Clearly G^0 is a finite irreducible nonsolvable subgroup of $\mathrm{Mon}(r, F)$ whenever G is. Since $G \leqslant G^0 Z$, it is reasonable to restrict our consideration to the case where G is contained in $\mathrm{Mon}(r, F)^0$.

We have a homomorphism π of $\mathrm{Mon}(r, F)$ onto S defined by replacing every nonzero entry in a monomial matrix by 1. The kernel of π is D. We note in passing that if F has characteristic $p > 0$, then 1 is the only p-power root of 1 in F and so D contains no nontrivial p-elements.

We are interested in classifying groups up to conjugacy in $GL(r, F)$. If G and $\widetilde{G}$ are subgroups of $\mathrm{Mon}(r, F)$, we write $G \sim \widetilde{G}$ if G is conjugate to $\widetilde{G}$ in $GL(r, F)$, and write $G \approx \widetilde{G}$ if they are conjugate under some element of $\mathrm{Mon}(r, F)$.

In what follows we shall refer to the following hypothesis:

(H) G is a finite nonsolvable irreducible subgroup of $\mathrm{Mon}(r, F)^0$ where r is a prime and F is an algebraically closed field. We define $A(G) := D \cap G$, $H := \pi(G)$, and H_1 as the stabilizer of e_1 in H.

Since G is nonsolvable and irreducible, H must be nonsolvable and transitive, so H_1 has index r in H. Conversely, given a transitive subgroup H of S, and a finite subgroup A of D^0 which is normalized by H, we define

$$\Delta(A, H) := \left\{ G \leqslant \mathrm{Mon}(r, F)^0 \mid \pi(G) = H \text{ and } A(G) = A \right\}$$

(we do *not* assume that the groups in $\Delta(A, H)$ are irreducible, but we shall see later that in most cases they are).

Our problem is to classify (up to conjugacy in $GL(r, F)$) the groups G which satisfy (H). This problem falls into three parts:

(I) Describe the permutation groups H which can arise for a specified prime r.
(II) Given a specific permutation group H of degree r, describe the possible subgroups A of D^0 which can occur as $A(G)$ for some G.
(III) Given H and A, describe $\Delta(A, H)$ and find representatives of the $\sim$-classes of groups in $\Delta(A, H)$.

Our main results on these questions are summarized below.

1.1. The possible factor groups H

Question (I) is easily answered using known results since H is transitive of prime degree. Based on the classification of finite simple groups, we have the following proposition.

Proposition 1.1 (see [9] or [6, p. 99]). *If H is a transitive nonsolvable subgroup of* $\mathrm{Sym}(r)$ *where r is a prime* (*necessarily $r \geqslant 5$*), *then H is 2-transitive and one of the following holds*:

(i) $\mathrm{Alt}(r) \leqslant H \leqslant \mathrm{Sym}(r)$ *with* $r \geqslant 5$;
(ii) $r \geqslant 5$ *has the form* $(q^n - 1)/(q - 1)$ *for some integer* $n \geqslant 2$ *and some prime power* q, *and* $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$; *or*
(iii) (*three exceptional cases*) $(r, H) = (11, PSL(2, 11))$, $(11, M_{11})$, *or* $(23, M_{23})$.

Case (i) with $r = 5$ is subsumed in (ii) with $(n, q) = (2, 4)$. The permutation representation in (ii) refers to the action on the set of lines of the underlying projective space. We can also consider the action on hyperplanes. For $n > 2$ these two representations are different, but the permutation groups they give rise to are conjugate in $\mathrm{Sym}(r)$ since the stabilizer of a line is mapped into the stabilizer of a hyperplane by a suitable outer automorphism (see Section 1.1.1 below).

For $PSL(2, 11)$ in (iii) there are also two conjugacy classes of subgroups of index 11, and hence two inequivalent permutation representations of degree 11. However, again the two classes are merged under an outer isomorphism so, up to conjugacy in $\mathrm{Sym}(r)$, the two representations have the same image. The one-point stabilizers in the three exceptional cases are isomorphic to $\mathrm{Alt}(5)$, $\mathrm{Alt}(6) \cdot 2$, and M_{22}, respectively.

Since we are interested in classifying the possible G up to conjugacy, we can assume that we have fixed arbitrarily one group $H \leqslant S$ for each permutation isomorphism class. Then Proposition 1.1 enables us to partition the set Π of all pairs (r, H) which arise for groups satisfying hypothesis (H) into three classes:

Π_1: all (r, H) with $r \geqslant 7$ and $H = \mathrm{Alt}(r)$ or $\mathrm{Sym}(r)$;
Π_2: all (r, H) with $r \geqslant 5$, $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$ and $r = (q^n - 1)/(q - 1)$ with the exception of $(7, PSL(3, 2))$;

Π_3: the exceptional cases $(r, H) = (7, PSL(3,2))$, $(11, PSL(2,11))$, $(11, M_{11})$, and $(23, M_{23})$.

Although this has not been proved, it is conjectured that Π_2 contains groups of infinitely many prime degrees; for example, every Mersenne prime r occurs. We shall see later why the pair $(7, PSL(3,2))$ has been moved from class Π_2 to class Π_3.

1.1.1. Permutation representation of $PSL(n,q)$

It helps to be a little more precise in identifying the permutation representation of $PSL(n,q)$ in class Π_2. A simple number theoretic argument (see [7, Lemma 3.1]) shows that, if $q = p^a$ where p is prime, then the primality of $r := (q^n - 1)/(q-1)$ implies that n is prime, $n \nmid q-1$ and $a \geqslant 1$ is a power of n. If $n = 2$ then $p = 2$ and r is a Fermat prime.

In particular, since $(n, q-1) = 1$, we have $PGL(n,q) = PSL(n,q) \cong SL(n,q)$, and $P\Gamma L(n,q)/PSL(n,q)$ is cyclic of order a (a power of n) (see [3, p. xvi]). Thus we may assume that the elements of H are identified with the matrices in $SL(n,q)$. The action considered is the action of H on lines (= 1-dimensional subspaces of $\mathbb{F}_q^n$). Without loss in generality we may assume that H_1 is the subgroup fixing the line spanned by $[1, 0, \ldots, 0]^\top$. It consists of the matrices of the form

$$\begin{bmatrix} \xi & w \\ 0 & y \end{bmatrix},$$

where $\xi \in \mathbb{F}_q^*$, w is a $1 \times (n-1)$ block, and $y \in GL(n-1,q)$ has determinant ξ^{-1}. The outer automorphism of H defined by $x \mapsto (x^{-1})^\top$ (the inverse transposed) maps H_1 onto the stabilizer of a hyperplane (= $(n-1)$-dimensional subspace). The outer automorphisms in $P\Gamma L(n,q)$ are obtained by applying Galois automorphisms from $\mathrm{Gal}(\mathbb{F}_q)$ to the entries of the matrices. The latter group is cyclic of order a (and hence a power of n from above), and is generated by the Frobenius mapping $\xi \mapsto \xi^p$. Under these hypotheses, $P\Gamma L(n,q)$ splits over $PSL(n,q)$.

1.2. The possible subgroups $A(G)$

We now turn to question (II). Suppose that $(r, H) \in \Pi$ is specified, and that G satisfies hypothesis (H) with $\pi(G) = H$. Now G acts by conjugation on D with $A(G)$ acting trivially. Thus we can consider D as a $\mathbb{Z}H$-module and we shall refer to any subgroup of D which is a $\mathbb{Z}H$-submodule as being an *H-stable* subgroup. In particular, D^0 and $A(G)$ are H-stable.

Conversely, if A is an H-stable subgroup of D^0, then AH is a subgroup of $\mathrm{Mon}(r, F)$. If A is not contained in Z, then Theorem 2.1 in Section 2 below shows that $(AH)^0$ is irreducible and hence satisfies hypothesis (H).

Thus to answer question (II) we must determine the lattice of finite H-stable subgroups of D^0. Since the Sylow subgroups of a finite H-stable group are also H-stable, it is enough to consider the H-stable subgroups of prime power orders.

For each integer $m > 0$ we define the H-stable subgroups $D(m) := \{u \in D \mid u^m = 1\}$ and $D^0(m) := D(m)^0$. Thus, if $\mathrm{char}(F) \nmid m$, then $D(m)$ is a direct product of r cyclic

groups of order m, and $|D^0(m)| = m^{r-1}$. (If $p = \mathrm{char}(F)$, then D contains no nontrivial p-subgroup.) Subgroups of the form $D^0(m)$ will be called *standard* subgroups.

Some important homomorphisms are related to these standard subgroups.

Definition 1.2. For each $x \in \mathrm{Mon}(r, F)$ we define $\varepsilon(x) := \det(\pi(x))$; hence $\varepsilon(x) = \pm 1$ depending on whether the permutation $\pi(x)$ is even or odd. For each integer m we define $\pi_m : \mathrm{Mon}(r, F) \to \mathrm{Mon}(r, F)$ by $\pi_m(x) := \varepsilon(x)^{m-1} x^{(m)}$ where $x^{(m)}$ is the matrix obtained from x by replacing each nonzero entry of x by its mth power. For each subgroup $K \leqslant \mathrm{Mon}(r, F)^0$ we define $\tilde{\pi}_m(K) := \pi_m^{-1}(K) \cap \mathrm{Mon}(r, F)^0$.

Lemma 1.3. *Let $m > 1$. Then*

(a) *π_m is a surjective homomorphism with kernel $D(m)$;*
(b) *π_m maps $\mathrm{Mon}(r, F)^0$ onto itself;*
(c) *$D^0(m) \leqslant \tilde{\pi}_m(K)$ for each $K \leqslant \mathrm{Mon}(r, F)^0$ and $\tilde{\pi}_m(K)/D^0(m) \cong K$.*

Proof. Statement (a) is clear (surjectivity follows from the fact that F is algebraically closed), so consider (b). For each $x \in \mathrm{Mon}(r, F)$, $\det(x) = \varepsilon(x)\delta$ where δ is the product of the nonzero entries in x and $\det(\pi_m(x)) = \varepsilon(x)^{r(m-1)+1}\delta^m = \varepsilon(x)^m \delta^m$ because r is odd. Thus $\det(\pi_m(x)) = \det(x)^m$. In particular, π_m maps $\mathrm{Mon}(r, F)^0$ into itself. Now suppose $y \in \mathrm{Mon}(r, F)^0$. By (a) we can choose $z \in \mathrm{Mon}(r, F)$ such that $\pi_m(z) = y$. Then $\det(z)^m = \det(y) = 1$ and so defining $u := \mathrm{diag}(\omega, 1, \ldots, 1)$ with $\omega = \det(z)^{-1}$, we have $x := uz \in \mathrm{Mon}(r, F)^0$ and $\pi_m(x) = 1$. This shows that π_m maps $\mathrm{Mon}(r, F)^0$ onto itself. This proves (b). Statement (c) now follows easily (apply π_m to $\tilde{\pi}_m(K)$). □

We call an H-stable subgroup of D^0 *basic* if it does not contain any $D^0(m) \neq 1$ and denote the set of finite basic H-stable subgroups of D^0 by $\Phi(r, H)$. If A is an H-stable subgroup of D^0, then it is clear that $\pi_m(A)$ and $\tilde{\pi}_m(A)$ are also H-stable since $\pi \circ \pi_m = \pi$. Each standard subgroup $D^0(m)$ has the form $\tilde{\pi}_m(1)$, and more generally every finite H-stable subgroup of D^0 can be written in the form $\tilde{\pi}_m(A)$ for some $m \geqslant 1$ and some $A \in \Phi(r, H)$. This representation is unique if we restrict m to be relatively prime to $\mathrm{char}(F)$ when the latter is nonzero. Thus a knowledge of $\Phi(r, H)$ completely determines the lattice of finite H-stable subgroups in D^0. Since each $A \in \Phi(r, H)$ is a direct product of its Sylow subgroups and these are all basic H-stable subgroups of prime power orders, it is enough to know the set $\Phi_p(r, H)$ of basic H-stable p-subgroups for each prime p. We shall see below (Theorem 1.5) that $\Phi(r, H)$ is always finite.

Remark. An alternative way to think about the lattice of finite H-stable subgroups is the following. Let H_1 be the stabilizer in H of the point e_1. Consider the multiplicative group F^* of the field F as a $\mathbb{Z}H_1$-module with trivial action. Then the permutation action of H is induced from this trivial module and so $D \cong \mathbb{Z}H \otimes_{\mathbb{Z}H_1} F^*$. Consider the analogous induced $\mathbb{Z}H$-module $M := \mathbb{Z}H \otimes_{\mathbb{Z}H_1} \mathbb{Z}$ where $\mathbb{Z}$ is the (additive!) $\mathbb{Z}H_1$-module with the trivial action. Then M as a $\mathbb{Z}$-module is free of rank $r = |H : H_1|$, and for each integer $m \geqslant 0$ with $\mathrm{char}(F) \nmid m$ we have $D(m) \cong M/mM$ as $\mathbb{Z}H$-modules. Hence the lattice $\mathcal{L}(M)$ of nonzero submodules of M determines the lattice of finite H-stable subgroups

of D. However, $\mathcal{L}(M)$ is independent of the field F and seems an important object to study in its own right.

For any integer $m > 0$ and prime p, π_m induces a $\mathbb{Z}H$-homomorphism of $D(mp)$ onto $D(p)$ with kernel $D(m)$. Therefore $D(mp)/D(m) \cong D(p)$ as $\mathbb{Z}H$-modules and similarly $D^0(mp)/D^0(m) \cong D^0(p)$. If $p = \mathrm{char}(F)$, then $D(p) = 1$, but if $p \neq \mathrm{char}(F)$, then $D(p) \cong \mathbb{F}_p H \otimes_{\mathbb{F}_p H_1} \mathbb{F}_p$ where $\mathbb{F}_p$ is the field with p elements (with $\mathbb{F}_p H_1$ acting trivially). Thus, when $p \neq \mathrm{char}(F)$, the structure of $D^0(mp)/D^0(m)$ is determined by the structure of this induced module. The latter is known and is described in the following proposition (adapted from [21] for the case where the degree is prime using the remarks at the beginning of Section 1.1.1).

Proposition 1.4 [21]. *Let H be a nonsolvable 2-transitive group of prime degree r (see Proposition 1.1) with a one-point stabilizer H_1. Let p be a prime and set $B_p := \mathbb{F}_p H \otimes_{\mathbb{F}_p H_1} \mathbb{F}_p$. If $p = r$, then B_p has a unique composition series of the form $0 < \mathbb{F}_p < B_p^0 < B_p$ where B_p^0 has codimension 1. On the other hand, if $p \neq r$, then we have the $\mathbb{F}_p H$-module decomposition $B_p = \mathbb{F}_p \oplus B_p^0$ where B_p^0 is irreducible except in the following cases*:

(i) $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$ *with* $n > 2$, $r = (q^n - 1)/(q - 1)$ *and* $p \mid q$;
(ii) $(r, H, p) = (11, PSL(2, 11), 3)$ *or* $(23, M_{23}, 2)$.

Remark. The submodule structure of B_p^0 in (i) can be quite complicated (see Section 3). In case (ii), when $H = PSL(2, 11)$ the module B_3^0 has a unique proper nonzero submodule of dimension 5 (see [21, p. 18]), and when $H = M_{23}$ the module B_2^0 has a unique proper nonzero submodule of dimension 11 (see [16]).

This proposition leads to the following theorem which is proved in Section 2.

Theorem 1.5. *Let $(r, H) \in \Pi$.*

(a) $\Phi_p(r, H) = \{1\}$ *for $p \neq r$ except in the cases listed in* (i) *or* (ii) *of Proposition* 1.4.
(b) $\Phi_r(r, H) = \{1, Z^0\}$.
(c) $\Phi_p(r, H)$ *is finite for all primes p, and hence $\Phi(r, H)$ is finite.*

1.3. The set of extensions $\Delta(A, H)$ of A by H

Given $(r, H) \in \Pi$ and a finite H-stable subgroup A of D^0, (III) asks for a classification of the extensions in $\Delta(A, H)$. Define $\widetilde{H} := \{\varepsilon(x)x \mid x \in H\}$ where $\varepsilon(x) = \pm 1$ depending on whether the permutation x is even or odd. Then $H \cong \widetilde{H} \leqslant \mathrm{Mon}(r, F)^0$ and $\pi(\widetilde{H}) = H$. Thus $G := A\widetilde{H} \in \Delta(A, H)$, and so this set of extensions is nonempty and contains at least one split extension.

In general, we can prove the following criterion for splitting.

Theorem 1.6. *Let G be a group which satisfies hypothesis* (H) *and put $d := |H_1 : H_1'|$. Then G splits over $A(G)$ whenever $|A(G)|$ is relatively prime to d.*

The proof will be given at the end of Section 4.

There is an important relationship between the sets $\Delta(A, H)$ and $\Delta(\tilde{\pi}_m(A), H)$ which turns out to be critical in our analysis (we are indebted to V. Burichenko who pointed this out to us).

Lemma 1.7 (V. Burichenko). *Let $H \leqslant S$ be a transitive group, and suppose that A and $\widetilde{A}$ are finite H-stable subgroups of D^0 such that for some positive integer m we have $\pi_m(\widetilde{A}) = A$.*

(a) *If $\widetilde{G}, \widetilde{K} \in \Delta(\widetilde{A}, H)$ and $\widetilde{G} \approx \widetilde{K}$, then $\pi_m(\widetilde{G}), \pi_m(\widetilde{K}) \in \Delta(A, H)$ and $\pi_m(\widetilde{G}) \approx \pi_m(\widetilde{K})$.*
(b) *If $\widetilde{A} := \tilde{\pi}_m(A)$, then π_m induces a bijection from $\Delta(\widetilde{A}, H)$ onto $\Delta(A, H)$ whose inverse is induced by $\tilde{\pi}_m$. Moreover, if $\widetilde{G}, \widetilde{K} \in \Delta(\widetilde{A}, H)$ then $\widetilde{G} \approx \widetilde{K}$ if and only if $\pi_m(\widetilde{G}) \approx \pi_m(\widetilde{K})$*

Proof. (a) It is clear that π_m maps $\Delta(\widetilde{A}, H)$ into $\Delta(A, H)$ since $\pi_m(\widetilde{A}) = A$, $\pi = \pi \circ \pi_m$, and π_m maps $\mathrm{Mon}(r, F)^0$ onto itself. Put $\pi_m(\widetilde{G}) = G$ and $\pi_m(\widetilde{K}) = K$. Since $\widetilde{G} \approx \widetilde{K}$, we have $\widetilde{G} = a^{-1}\widetilde{K}a$ for some $a \in \mathrm{Mon}(r, F)$. Thus $G = \pi_m(a)^{-1}K\pi_m(a)$ and so $G \approx K$.

(b) As we saw in (a), π_m maps $\Delta(\widetilde{A}, H)$ into $\Delta(A, H)$. Now for each $G \in \Delta(A, H)$, the inverse image $\widetilde{G} := \tilde{\pi}_m(G) \in \Delta(\widetilde{A}, H)$, and $\pi_m(\widetilde{G}) = G$. Since every group in $\Delta(\widetilde{A}, H)$ which maps onto G must be contained in this inverse image and all groups in $\Delta(\widetilde{A}, H)$ have the same order, this shows that $\widetilde{G}$ is the only group in $\Delta(\widetilde{A}, H)$ which maps onto G. Hence π_m induces a bijection and the inverse of this bijection is induced by $\tilde{\pi}_m$.

Now suppose that $\widetilde{G}, \widetilde{K} \in \Delta(\widetilde{A}, H)$ and put $\pi_m(\widetilde{G}) = G$ and $\pi_m(\widetilde{K}) = K$. We saw in (a) that $\widetilde{G} \approx \widetilde{K}$ implies that $G \approx K$. Conversely, if $G = b^{-1}Kb$ for some $b \in \mathrm{Mon}(r, F)$, then $\widetilde{G} = a^{-1}\widetilde{K}a$ for any $a \in \tilde{\pi}(b)$ since $\widetilde{G} = \tilde{\pi}_m(G)$. □

Since every H-stable subgroup is of the form $\tilde{\pi}_m(A)$ for some basic H-stable subgroup A and some $m \geqslant 1$, the lemma above reduces the problem of describing $\Delta(A, H)$ and its $\approx$-classes to the case where A is basic. As Lemma 2.1 below shows, the $\sim$-classes and $\approx$-classes of $\Delta(A, H)$ coincide whenever A is noncentral.

At this point the reader might find it helpful to look at the final section of this paper where our description of the extensions corresponding to a fixed pair $(r, H) \in \Pi$ is worked out in detail for particular cases.

2. Some general results

Recall that $\Omega = \{e_1, \ldots, e_r\}$ is the standard basis of the underlying vector space F^r so that the subspaces $Fe_1, \ldots, Fe_r$ are permuted under the action of $\mathrm{Mon}(r, F)$. We start with the following elementary result.

Lemma 2.1.

(a) *Let G be a subgroup of* $\mathrm{Mon}(r, F)^0$ *where r is a prime and F is an algebraically closed field. Suppose that $H := \pi(G)$ is a transitive group and $A(G) := G \cap D$ is not a group of scalars. Then G is irreducible* (*and so satisfies hypothesis* (H) *if H is nonsolvable*).

(b) *Suppose that G and $\widetilde{G}$ are two groups which satisfy hypothesis* (H) *and $A(G)$ and $A(\widetilde{G})$ are both nonscalar. If G and $\widetilde{G}$ are conjugate in $GL(r, F)$ then they are also conjugate in* $\mathrm{Mon}(r, F)$.

Remark. As we shall see in Section 5 both conclusions may be false when the abelian normal subgroup is scalar.

Proof. (a) There exist r one-dimensional representations λ_i of $A(G)$ defined by $xe_i = \lambda_i(x)e_i$ for all $x \in A(G)$. Consider the equivalence relation ρ on Ω defined by $e_i \,\rho\, e_j \Leftrightarrow \lambda_i = \lambda_j$. This relation is invariant under H. Since H is transitive on Ω and r is prime, the ρ-equivalence classes must all have the same size and so either the λ_i are distinct or all equal. The latter is impossible since $A(G)$ is nonscalar, and so $\lambda_i \neq \lambda_j$ whenever $i \neq j$. This implies that $Fe_1, \ldots, Fe_r$ are the only minimal $A(G)$-invariant subspaces of F^r. Thus any nonzero G-invariant subspace contains some Fe_i and so contains them all by the transitivity of H. This shows that G is irreducible.

(b) Choose $c \in GL(r, F)$ such that $c^{-1}Gc = \widetilde{G}$. Then $c^{-1}A(G)c = A(\widetilde{G})$ because $A(G)$ and $A(\widetilde{G})$ are the unique maximal normal abelian subgroups of G and $\widetilde{G}$, respectively. As we saw in (a), $Fe_1, \ldots, Fe_r$ are the unique minimal invariant subspaces for both $A(G)$ and $A(\widetilde{G})$. Hence c must permute this set of subspaces and so $c \in \mathrm{Mon}(r, F)$. □

If G is a subgroup of $\mathrm{Mon}(r, F)$ such that $H := \pi(G)$ is transitive (but not necessarily nonsolvable), then G permutes the set of 1-dimensional subspaces $Fe_1, \ldots, Fe_r$ transitively. Let G_i be the subgroup (of index r in G) which fixes the space Fe_i, so $H_i := \pi(G_i)$ is the stabilizer of e_i in H. Then we have a representation λ_i of degree 1 for G_i defined by $xe_i = \lambda_i(x)e_i$ for all $x \in G_i$. Note that the kernel of λ_i contains G_1'. Since $\lambda_i(G_i)$ is a finite subgroup of the multiplicative group F^* of the field, $\lambda_i(G_i)$ is cyclic, and so $|\lambda_i(G_i)|$ divides the exponent of G_i/G_i'.

Lemma 2.2. *Let G be a subgroup of* $\mathrm{Mon}(r, F)$ *such that $H := \pi(G)$ is transitive and let d be the exponent of the group G_1/G_1'. Then G is conjugate in* $\mathrm{Mon}(r, F)$ *to a group K such that K contains an r-cycle from S and the nonzero entries of every element of K are all dth roots of* 1 *in F.*

Proof. Because H is transitive, we can choose $z \in G$ such that $z_0 := \pi(z)$ is an r-cycle. Conjugating if necessary by a permutation matrix, we can assume z_0 corresponds to the permutation $(1\,2\,\ldots\,r)$ and $z = \mathrm{diag}(\alpha_1, \ldots, \alpha_r)z_0$. Since $\det(z) = 1$, a simple calculation shows that

$$\mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_r)^{-1} z\, \mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_r) = z_0,$$

where $\beta_i = a_i\alpha_{i+1}\dots\alpha_r$ (for $i = 1,\dots,r$). Thus, there exists $c \in \mathrm{Mon}(r,F)$ such that $z_0 := c^{-1}zc \in S$. We claim that the nonzero entries of all matrices in $K := c^{-1}Gc$ are dth roots of 1.

Now suppose that $x \in K$ and that $xe_i = \zeta e_j$ for some i and j. We have to show that $\zeta^d = 1$. Since z_0 is an r-cycle, we can choose an integer l such that $z_0^l e_j = e_i$ and then $z_0^l x e_i = \zeta e_i$. Thus with the notation above, $\zeta \in \lambda_i(K_i)$ and so the order of ζ divides the exponent of K_i/K_i'. Since the subgroups $K_1,\dots,K_r$ are conjugate in K by the transitivity of H and $K_1/K_1' \cong G_1/G_1'$, the result follows. □

As a simple application of the last two lemmas we have the following useful criteria for splitting.

Theorem 2.3. *Suppose that G is a group satisfying hypothesis* (H). *Then*

(a) *G splits over the Sylow r-subgroup A_r of $A(G)$ and every pair of complements of A_r in G are conjugate in* $\mathrm{Mon}(r,F)$;
(b) *if $A(G) = A_r D^0(m)$ for some $m \geqslant 1$ where m is relatively prime to $|H_1 : H_1'|$, then G splits over $A(G)$.*

Proof. (a) The previous lemma shows that without loss in generality we can assume that G contains an r-cycle z from S. Note that $\langle z\rangle$ is a Sylow r-subgroup of H. Hence, if R is a Sylow r-subgroup of G containing z, then $R = A_r(R \cap S)$ where $R \cap S = \langle z\rangle$ and so R splits over A_r. Therefore Gaschütz' theorem (see, for example, [13, p. 121]) shows that G splits over A_r.

Next, let D_r be the Sylow r-subgroup of the infinite group D. If L is another complement of A_r in R, then L is a complement of D_r^0 in $D_r^0\langle z\rangle$. Since $L = \langle w\rangle$ for some w for which $\pi(w) = z$ and the nonzero entries of w are r-power roots of 1, the calculation in the proof of Lemma 2.2 shows that w is conjugate to z under some element c in D_r. Multiplying by a suitable scalar and using the fact that F is algebraically closed, we can replace c by an element in D_r^0. Since $D_r^0\langle z\rangle$ is a Sylow r-subgroup of D_r^0G and the complements of D_r^0 in $D_r^0\langle z\rangle$ are conjugate in $D_r^0\langle z\rangle$, the second part of Gaschütz' theorem shows that every complement of D_r^0 in D_r^0G is conjugate to $\langle z\rangle$ in D_r^0G. Hence the complements of A_r in G are conjugate in $\mathrm{Mon}(r,F)$.

(b) G splits over A_r by part (a), so it is enough to prove (b) when $A(G) = D^0(m)$. Since $H_1/H_1' \cong G_1/G_1'A(G)$, the exponent of G_1/G_1' divides mk where $k := |H_1 : H_1'|$. Hence by Lemma 2.2 we can assume that the nonzero entries in the matrices in G are all (mk)th roots of 1. However $G \cong \pi_k(G)$ since $A(G) \cap D(k) = 1$ by hypothesis, and the nonzero entries in the matrices in $\pi_k(G)$ are all mth roots of 1. In general, $K := \pi_k(G)$ need not lie in $SL(r,F)$. However, $K^0 \geqslant D^0(m)$, and so $|K : K^0|$ clearly divides $|H_1 : H_1'| = k$. Thus $|K : K^0|$ is relatively prime to m. Now Gaschütz' theorem shows that if K^0 splits over $A(K^0)$ $(= D^0(m))$, then K (and hence G) also splits over $D^0(m)$. Thus (replacing G by K^0) it is enough to prove the result in the case that the nonzero entries in the matrices in G are all mth roots of 1.

Now $\widetilde{H} := \{\varepsilon(x)x \mid x \in H\} = \pi_m(G)$ is isomorphic to H and lies in $\Delta(1,H)$. Hence $D^0(m)\widetilde{H}$ and G both lie in $\Delta(D^0(m),H)$ and are mapped onto the same group $\widetilde{H}$ in

$\Delta(1, H)$ by π_m. Thus Lemma 1.7 shows that $G = D^0(m)\widetilde{H}$ which gives the required splitting. □

We now turn to a proof of Theorem 1.5 in the Introduction. We begin with a lemma.

Lemma 2.4. *If A is an H-stable subgroup of $D^0(p^{k+1})$, then $AD^0(p^k)/D^0(p^k) \simeq \pi_p(A)D^0(p^{k-1})/D^0(p^{k-1})$ as H-modules. Moreover, if $AD^0(p^k) = D^0(p^{k+1})$, then $A = D^0(p^{k+1})$.*

Proof. The first statement follows at once from consideration of the H-homomorphism $A \to D^0(p^k)/D^0(p^{k-1})$ defined by $u \mapsto \pi_p(u)D^0(p^{k-1})$.

To prove the second statement we use induction on k. The statement is trivially true for $k = 0$, so suppose $k > 0$. Now applying π_p to both sides of $AD^0(p^k) = D^0(p^{k+1})$ gives $\pi_p(A)D^0(p^{k-1}) = D^0(p^k)$. Thus $A \geqslant \pi_p(A) = D^0(p^k)$ by the inductive hypothesis. Hence $A = AD^0(p^k) = D^0(p^{k+1})$ as required. □

2.1. Proof of Theorem 1.5

(a) Suppose that $p \neq r$ and assume that the exceptional cases (i) and (ii) of Proposition 1.4 do not hold. We have to show that every H-stable p-subgroup is of the form $\tilde{\pi}_{p^k}(1)$. Let A be any H-stable p-subgroup of D^0, and assume that $A \leqslant D^0(p^{k+1})$ but $A \not\leqslant D^0(p^k)$. Since $D^0(p^{k+1})/D^0(p^k) \cong B_p^0$ is irreducible by Proposition 1.4, therefore $AD^0(p^k) = D^0(p^{k+1})$. Now Lemma 2.4 shows that $A = D^0(p^{k+1}) = \tilde{\pi}_{p^{k+1}}(1)$. Hence $\Phi_p(r, H) = \{1\}$ as required.

(b) Now consider the case $p = r$. A simple calculation shows that $\tilde{\pi}_{r^k}(Z^0) = D^1(r^k) := ZD(r^k) \cap D^0(r^{k+1})$ and $|D^1(r^k)| = r|D^0(r^k)|$ (recall that Z is the group of scalars). Thus to prove (b) it is enough to show that if A is an H-stable r-subgroup of D^0 such that $A \leqslant D^0(r^{k+1})$ but $A \not\leqslant D^0(r^k)$ then either $A = D^0(r^{k+1})$ or $D^1(r^k)$. If $A = D^0(r^{k+1})$, we are finished. Otherwise, we know from Proposition 1.4 that B_r^0 has only one proper nonzero submodule. Since $D^0(r^{k+1})/D^0(r^k) \simeq B_r^0$, this shows that $AD^0(r^k) = D^1(r^k)$.

To complete the proof we must show that

$$AD^0\big(r^k\big) = D^1\big(r^k\big) \quad \text{implies that} \quad A = D^1\big(r^k\big) \tag{1}$$

for all k. This is trivial if $k = 0$ so consider the case $k = 1$. Choose $u \in D^1(r) \setminus D^0(r)$ lying in A. Then u has order r^2 and determinant 1, so u is not scalar. Hence u has two diagonal entries, say the ith and jth which are not equal. Since H is 2-transitive by Proposition 1.1, we can choose $x \in H$ which maps i into j and fixes some l. Now $v := x^{-1}u^{-1}xu \in A$ is not scalar so $v \notin D^1(1)$. On the other hand, since H centralizes $D^1(r)/D^0(r)$, we have $v \in D^0(r) \cap A$. Since $D^0(r) \cong B_r^0$, Proposition 1.4 shows that $D^1(1)$ is the only proper nontrivial H-stable subgroup of $D^0(r)$. But $v \notin D^1(1)$, so $D^0(r) \leqslant A$ and hence $A = AD^0(r) = D^1(r)$ as required. This proves the case $k = 1$.

Finally, we use induction to prove the case $k \geqslant 2$. We are given that $AD^0(r^k) = D^1(r^k)$. Applying π_r to both sides gives $\pi_r(A)D^0(r^{k-1}) = D^1(r^{k-1})$, and then induction shows

that $D^1(r^{k-1}) = \pi_r(A)$ and hence $D^0(r^{k-1}) \leqslant A$. Thus $D^1(r) = \pi_{r^{k-1}}(A) \cong A/D^0(r^{k-1})$. Since $A \leqslant D^1(r^k)$, a comparison of orders shows that $A = D^1(r^k)$.

(c) We want to show that $\Phi(r, H)$ is always finite and so, in principle, we always have a simple description of the finite H-stable subgroups. In practice, it may be difficult to determine what this set is. Since each basic subgroup is a direct product of its Sylow subgroups which are also basic, and $\Phi_p(r, H) = \{1\}$ for all but at most one prime other than r, it is enough to prove that $\Phi_p(r, H)$ is finite for each prime p.

Let A be a finite H-stable p-subgroup of D^0. We shall say that A has *height* k if $A \leqslant D^0(p^k)$ but $A \not\leqslant D^0(p^{k-1})$. If A has height k, then we have a series of H-stable subgroups

$$A = A_k \geqslant A_{k-1} \geqslant \cdots \geqslant A_0 = 1 \quad \text{with } A_i := A \cap D^0\big(p^i\big) \text{ for each } i. \tag{2}$$

It follows from Lemma 2.4 that the factors $A_i/A_{i-1} \cong U_i$ where U_i is a submodule of B_p^0 and

$$U_k \leqslant U_{k-1} \leqslant \cdots \leqslant U_1. \tag{3}$$

The H-stable p-subgroup A will be called *U-homogeneous* if each of the U_i is isomorphic to U. We note that $A/A_1 \cong \pi_p(A) \leqslant A_{k-1}$. Thus, when A is U-homogeneous, a comparison of orders shows that $\pi_p(A) = A_{k-1}$. The key step in the proof that $\Phi_p(r, H)$ is finite is the following result.

Lemma 2.5. *Let $p \neq \mathrm{char}(F)$ be a prime and suppose that p^e is the largest power of p dividing $|H|$. Then for each proper nonzero submodule U of B_p^0 the height of every U-homogeneous H-stable p-subgroup is bounded by $2e$.*

Proof. Let $\mathbb{D}_p$ denote the ring of p-adic integers and $\mathbb{Q}_p$ the field of p-adic numbers. Consider the $\mathbb{D}_p H$-module $M := (\mathbb{D}_p)^r$ where the action of H on M is via matrix multiplication. This module has a submodule M^0 (of codimension 1) consisting of all vectors whose components sum to 0, and thus M is isomorphic to the $\mathbb{D}_p H$-module induced from the trivial $\mathbb{D}_p H_1$-module. Since $\mathrm{char}(\mathbb{D}_p) = 0$ and H is 2-transitive, $M \otimes \mathbb{Q}_p$ has only two proper nonzero submodules and so $M^0 \otimes \mathbb{Q}_p$ is (absolutely) irreducible (see [13, p. 597]).

Let A be a U-homogeneous H-stable p-subgroup of height k. Let ζ be a primitive p^kth root of 1 in F. Then

$$(m_1, \ldots, m_r) \mapsto \mathrm{diag}\big(\zeta^{m_1}, \ldots, \zeta^{m_r}\big)$$

defines a $\mathbb{D}_p H$-homomorphism of M^0 onto $D^0(p^k)$ with kernel $p^k M^0$ (note that ζ^m is well-defined for $m \in \mathbb{D}_p$ because ζ is a p-power root of 1). Let V be the inverse image of A under this homomorphism. Since $p^i M^0$ is the inverse image of $D^0(p^{k-i})$ for $i = 0, 1, \ldots, k$, therefore $(V \cap p^i M^0)/(V \cap p^{i+1} M^0) \cong A_{k-i}/A_{k-i-1} \cong U$ for $i = 0, 1, \ldots, k-1$. Now choose $u_1, \ldots, u_{r-1}$ in M^0 such that $u_i + pM^0$ $(i = 1, \ldots, r-1)$ is a basis for the vector space M^0/pM^0 with the first d, say, of the elements lying in V such

that $u_i + pM^0$ $(i = 1, \ldots, d)$ is a basis for $(V + pM^0)/pM^0$ $(\cong U)$. Since V/p^kM^0 is U-homogeneous, the elements $u_i + p^kM^0$ $(i = 1, \ldots, d)$ generate all of V/p^kM^0. Since $\mathbb{D}_p$ is local, Nakayama's lemma shows that $u_1, \ldots, u_{r-1}$ generate M^0 as a $\mathbb{D}_p$-module. Since M^0 is irreducible, [4, Theorem 76.11] (together with the remarks following Theorem 75.19) now show that $k \leqslant 2e$ as claimed. □

We can now complete the proof that $\Phi_p(r, H)$ is finite for each prime p. Suppose the contrary. Then there are basic p-subgroups of arbitrarily large height. Since B_p^0 is finite, it follows from the series (2) and (3) that there exists a proper nonzero submodule U of B_p^0 and a basic p-subgroup A such that for some s and t with $t - s > 2e$ we have $U_i \cong U$ for $i = s + 1, s + 2, \ldots, t$. But now $\pi_{p^s}(A_t)$ is a U-homogeneous basic p-subgroup of height $t - s > 2e$ and this is impossible by the previous lemma.

3. H-stable p-subgroups when $H = PSL(n, q)$ and $p \mid q$

Suppose that G satisfies the hypothesis (H) and $p \neq r$. Then Theorem 1.5(a) shows that the H-stable p-subgroups are all standard except when either $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$, $r = (q^n - 1)/(q - 1)$, and $p \mid q$, or $(r, H, p) = (11, PSL(2, 11), 3)$ or $(23, M_{23}, 2)$. We shall consider the latter exceptions in Section 6.3.

We shall start by considering the problem of describing the $PSL(n, q)$-stable p-subgroups when $p \mid q$. However, we shall see below (Corollary 3.8) that these p-subgroups remain stable under H whenever $PSL(n, q) < H \leqslant P\Gamma L(n, q)$, and so the same description is valid for H-stable p-subgroups in the more general case.

Recall that primality of r implies that $(n, q - 1) = 1$ and so $PSL(n, q) \cong PGL(n, q) \cong SL(n, q)$ (see the remark following Proposition 1.1).

3.1. The structure of B_p

Unless stated otherwise, the results in this subsection are valid whenever $H = SL(n, q)$ and $q = p^a$ for some prime p and integer $a \geqslant 1$ (without the restriction that $(q^n - 1)/(q - 1)$ is prime). As we shall see in Corollary 3.8 below, under hypothesis (H) our results will apply more generally to all H with $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$.

The lattice of H-stable p-subgroups is largely determined by the structure of the $\mathbb{F}_pH$-module $B_p := \mathbb{F}_pH \otimes_{\mathbb{F}_pH_1} \mathbb{F}_p$ induced from the trivial module $\mathbb{F}_p$ for the stabilizer H_1 of a line (in other words, B_p is the permutation module of H acting on the set of lines). We could also consider the corresponding module induced from the trivial module for the stabilizer of a hyperplane; the two modules are dual and have the same submodule lattice.

The composition factors of B_p for $p > 2$ were determined in [31]. More recently, a complete description of the submodules of B_p was determined in [2]. We recall these results here and interpret them for our problem.

Let V be the natural $\mathbb{F}_qL$-module where $L := GL(n, q)$ and $q = p^a$. It is convenient to extend the scalars to the algebraic closure $\mathbb{E}$ of $\mathbb{F}_q$. Let X be the polynomial ring

$\mathbb{E}[x_1, \ldots, x_n]$ and let $X_p := X/\langle x_1^p, \ldots, x_n^p \rangle$ be the quotient over the ideal generated by pth powers of $x_1, \ldots, x_n$. We identify $V \otimes \mathbb{E}$ with the space of linear polynomials

$$V \otimes \mathbb{E} := \{a_1 x_1 + \cdots + a_n x_n \mid a_1, \ldots, a_n \in \mathbb{E}\}.$$

The action of L on $V \otimes \mathbb{E}$ extends to X in a natural way and, since $\langle x_1^p, \ldots, x_n^p \rangle$ is an L-invariant ideal, this action is inherited by X_p. Let $X(i)$ be the image in X_p of the space of the homogeneous polynomials of degree i in X (the space of "truncated polynomials of degree i"). Thus $X(i)$ is an $\mathbb{E}L$-module and it is clear that $X(i) \neq 0$ for $i = 0, 1, \ldots, n(p-1)$. In particular, $X(n(p-1))$ is a 1-dimensional space spanned by $x_1^{p-1} \cdots x_n^{p-1}$. If $p = 2$ then $X(i)$ is just the ith exterior power of the natural module. The following is known (recall that the term "infinitesimally irreducible" means that the $SL(n, q)$-module remains irreducible under restriction to $SL(n, p)$).

Lemma 3.1 (see [30]). *For each $i \leqslant n(p-1)$, $X(i)$ is an infinitesimally irreducible $\mathbb{E}SL(n, q)$-module and $X(i)$ and $X(n(p-1)-i)$ are dual. If $n > 2$, then the $X(i)$ are nonisomorphic except for the pair $X(0) \cong X(n(p-1))$.*

C.W. Curtis and R. Steinberg have shown how to use the modules $X(i)$ to construct a family of irreducible $\mathbb{E}L$-modules as follows. Let σ be the Frobenius automorphism of $\mathbb{E}$ (so $\sigma(\alpha) = \alpha^p$ for $\alpha \in \mathbb{E}$). We can extend σ in a natural way to an automorphism of $GL(n, q)$ which we also denote by σ. Let $Fr\, X(i)$ denote the σ-twist of $X(i)$ (the module is the same space but the action of L is twisted by applying σ). Then:

Lemma 3.2 (see [27, Theorems 41 and 43]). *Let $q = p^a$. Then for all a-tuples $(i_1, \ldots, i_a)$ with $0 \leqslant i_1, \ldots, i_a < n(p-1)$ the $\mathbb{E}L$-modules*

$$X(i_1, \ldots, i_a) := X(i_1) \otimes Fr\, X(i_2) \otimes \cdots \otimes Fr^{a-1}\, X(i_a)$$

are irreducible and pairwise inequivalent.

Theorem 3.3 (see [31, Theorem 1.6]). *Let $q = p^a$. Then the $\mathbb{E}L$-irreducible constituents of $B_p \otimes \mathbb{E}$ are precisely the modules of the form $X(i_1, \ldots, i_a)$ where $i_1 + i_2 p + \cdots + i_a p^{a-1} \equiv 0 \pmod{q-1}$.*

This result was extended by Bardoe and Sin [2] who give a complete determination of the $\mathbb{E}L$-submodules of $B_p \otimes \mathbb{E}$ as follows.

Consider the set $\mathcal{H}$ consisting of all a-tuples $(s_0, \ldots, s_{a-1})$ of integers which for all j satisfy: (i) $1 \leqslant s_j \leqslant n-1$; and (ii) $0 \leqslant ps_{j+1} - s_j \leqslant (p-1)n$ (taking subscripts modulo a). Define a partial ordering $\preccurlyeq$ on $\mathcal{H}$ by: $(s'_0, \ldots, s'_{a-1}) \preccurlyeq (s_0, \ldots, s_{a-1}) \Leftrightarrow s'_j \leqslant s_j$ for all j. An order ideal of $(\mathcal{H}, \preccurlyeq)$ is a subset $\mathcal{I}$ of $\mathcal{H}$ such that $(s_0, \ldots, s_{a-1}) \in \mathcal{I}$ and $(s'_0, \ldots, s'_{a-1}) \preccurlyeq (s_0, \ldots, s_{a-1})$ implies that $(s'_0, \ldots, s'_{a-1}) \in \mathcal{I}$. For each $(s_0, \ldots, s_{a-1}) \in \mathcal{H}$ we define $L(s_0, \ldots, s_{a-1}) := X(i_1, \ldots, i_a)$ where $i_j := ps_j - s_{j-1}$ (taking subscripts modulo a). (A simple combinatorial argument shows that the a-tuples

$(i_1, \ldots, i_a)$ which can be derived in this way are precisely those which satisfy the criterion in Theorem 3.3.)

Let $\widetilde{B}_p$ denote the permutation module for $GL(n, q)$ acting on the set of $(q^n - 1)/(q - 1)$ lines. As before we can write $\widetilde{B}_p = \mathbb{E} \oplus \widetilde{B}_p^0$ and we are interested in the structure of the submodule $\widetilde{B}_p^0$.

Theorem 3.4 (see [2, Theorem A]). *The $\mathbb{E}GL(n, q)$-module $\widetilde{B}_p^0$ is multiplicity-free* (*and so has only a finite number of submodules*) *and its composition factors are $L(s_0, \ldots, s_{a-1})$ where $(s_0, \ldots, s_{a-1}) \in \mathcal{H}$. If the composition factors of a submodule M of $\widetilde{B}_p^0$ are parametrized by the set $\mathcal{H}_M$, then $\mathcal{H}_M$ is an order ideal of $(\mathcal{H}, \preccurlyeq)$. The mapping $M \mapsto \mathcal{H}_M$ defines a lattice isomorphism $M \mapsto \mathcal{H}_M$ from the lattice of submodules of $\widetilde{B}_p^0$ to the lattice of order ideals of $(\mathcal{H}, \preccurlyeq)$.*

The submodule $L(0, \ldots, 0)$ is the submodule $\mathbb{E}$ of dimension 1 with trivial action which is a direct summand of $\widetilde{B}_p$. Note that the centre of $GL(n, q)$ acts trivially on $\widetilde{B}_p$, so the latter can be considered as an $\mathbb{E}PGL(n, q)$-module.

We now assume that $PSL(n, q) \cong PGL(n, q)$ (which holds in the case we are interested in) and so $\widetilde{B}_p$ is an $\mathbb{E}H$-module. In order to go from the submodules of $\widetilde{B}_p$ to the $\mathbb{F}_p H$-submodules of B_p, we use the following well-known result (see, for instance, [4, Theorem 70.15]).

Lemma 3.5. *Let M be an irreducible $\mathbb{F}_p H$-module. Then the irreducible $\mathbb{E}H$-constituents of $M \otimes \mathbb{E}$ have multiplicity* 1 *and are conjugate to each other under automorphisms from $\langle \sigma \rangle$ extended to $GL(M \otimes \mathbb{E})$.*

Thus $X(i_1, \ldots, i_a)$ is an $\mathbb{F}_p H$-module if and only if it is fixed by Fr. In general, $X(i_1, \ldots, i_a)$ is a constituent of $M \otimes \mathbb{E}$ for some irreducible $\mathbb{F}_p H$-module M, and $M \otimes \mathbb{E}$ is equal to the sum of pairwise distinct $\mathbb{E}H$-modules of the form $Fr^j X(i_1, \ldots, i_a)$.

The definition of $X(i_1, \ldots, i_a)$ shows that $Fr\, X(i_1, \ldots, i_a) = X(i_a, i_1 \ldots, i_{a-1})$ (a cyclic permutation). Thus $X(i_1, \ldots, i_a)$ and $X(j_1, \ldots, j_a)$ are $\mathbb{E}H$-components of the same irreducible $\mathbb{F}_p H$-module if and only if $(i_1, \ldots, i_a)$ and $(j_1, \ldots, j_a)$ differ only by a cyclic permutation. In particular, $X(i_1, \ldots, i_a)$ is an $\mathbb{F}_p H$-module if and only if $i_1 = \cdots = i_a$.

Let $[s_0, \ldots, s_{a-1}]$ be the class of all elements in $\mathcal{H}$ which are cyclic permutations of $(s_0, \ldots, s_{a-1})$. Examining the definition of $L(s_0, \ldots, s_{a-1})$ above, we obtain the following theorem.

Theorem 3.6. *Suppose hypothesis* (H) *holds and that $H = PSL(n, q)$ where $r := (q^n - 1)/(q - 1)$ is prime and $q = p^a$. Then the irreducible $\mathbb{F}_p H$-constituents of B_p^0 are parametrized by the classes $[s_0, \ldots, s_{a-1}]$ where $(s_0, \ldots, s_{a-1}) \in \mathcal{H}$. The lattice of $\mathbb{F}_p H$-submodules of B_p^0 is isomorphic to the lattice of order ideals of $\mathcal{H}$ which consist of unions of these classes.*

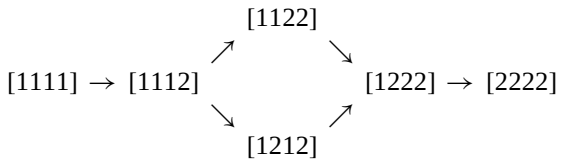
Corollary 3.7. *The socle of B_p^0 is $X((p-1)(n-1),\dots,(p-1)(n-1))$ and the head* (= *cosocle*) *is $X(p-1,\dots,p-1)$. These are dual by Lemma* 3.1. *When $n=2$, $\mathcal{H}$ has only one element, so B_p^0 is irreducible* (*as is well known*).

If we had considered the permutation module acting on the set of hyperplanes, then the head and socle would be interchanged.

It follows from Section 1.1.1 that under hypothesis (H) $P\Gamma L(n,q)$ is the extension of $PSL(n,q)$ by Γ where Γ is the group of automorphisms induced by field automorphisms of $\mathbb{F}_q$. Since each $\mathbb{F}_pPSL(n,q)$-submodule of B_p^0 is invariant under Fr, this gives the following useful result.

Corollary 3.8. *Every $\mathbb{F}_pPSL(n,q)$-submodule of B_p^0 is also an $\mathbb{F}_pP\Gamma L(n,q)$-submodule, and so every finite $PSL(n,q)$-stable p-subgroup of D^0 is $P\Gamma L(n,q)$-stable.*

Example 3.9. Theorem 3.6 shows that if $a=1$, then the $\mathbb{F}_pH$-submodules of B_p^0 form a chain (this was observed earlier in [22]). However, in general, when $a>1$ and $n>1$ the lattice of $\mathbb{F}_pH$-submodules of B_p^0 need not form a chain. For example, if $(n,q)=(3,2^4)$, then we get the lattice



(the sizes of the modules increases from left to right). Of course, in this case $r:=(q^n-1)/(q-1)$ is not prime. The smallest example where r is prime and the lattice is not a chain occurs when $(n,q)=(3,2^9)$ and $r=262657$.

The module $X(j_1,\dots,j_a)$ has dimension equal to $\prod_{k=1}^a \dim X(j_k)$. In [15] (or [14, Chapter VIII, Theorem 2.10]) it is shown that $\dim X(j)$ is the coefficient of t^j in the product $(1+t+t^2+\cdots+t^{p-1})^n$. (Another formula for $\dim X(j_k)$ can be found in Bardoe and Sin [2, Corollary 2.1].) When $j<p$ this coefficient is equal to $\binom{n+j-1}{j}$. In particular, $\dim X(p-1)=(n+p-2)!/(p-1)!(n-1)!$ and so

$$\dim X(p-1,\dots,p-1)=\bigl\{(n+p-2)!/(p-1)!(n-1)!\bigr\}^a.$$

Since the modules $X(p-1,\dots,p-1)$ and $X((n-1)(p-1),\dots,(n-1)(p-1))$ are dual, their dimensions are equal. This implies the following proposition.

Proposition 3.10. *Suppose hypothesis* (H) *holds, and $H=PSL(n,q)$ with $r=(q^n-1)/(q-1)$ and $q=p^a$. If the Sylow p-subgroup of $A(G)$ is nontrivial, then G contains a unique minimal normal p-subgroup K. The order of K is p^k where $k:=((n+p-2)!)^a/((p-1)!(n-1)!)^a$ and so $|A(G)|$ is a multiple of p^k.*

Proof. By hypothesis, $A(G) \cap D^0(p) \neq 1$ and it contains every minimal normal p-subgroup of G. On the other hand, $B_p = \mathbb{F}_p \oplus B_p^0$ (see Proposition 1.4) and $D^0(p) \cong B_p^0$ as H-modules. Since B_p^0 has a unique minimal normal submodule isomorphic to $M := X((p-1)(n-1), \ldots, (p-1)(n-1))$ by Corollary 3.7, we conclude that $A(G) \cap D^0(p)$ contains a unique minimal normal subgroup K of G corresponding to M. The order of K is p^k where $k = \dim M$ and this was calculated above. □

3.2. *H-stable p-subgroups*

Now assume that $(r, H) \in \Pi_2$ with $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$ and $q = p^a$. To avoid the trivial case assume that $p \neq \mathrm{char}(F)$. Corollary 3.8 shows that the lattice of H-stable p-subgroups of D^0 is the same as the lattice of $PSL(n, q)$-stable p-subgroups, so without loss in generality we can take $H = PSL(n, q)$.

Every finite H-stable p-subgroup A has a series of the form (2) and (3) where the U_i are submodules of B_p^0, but as we saw in Section 2.1 not every series of this form can occur. In general, we have not been able to characterise the basic H-stable p-subgroups in this case, but some special cases can be dealt with. For example, when $n = 2$, we must have $p = 2$ and r is a Fermat prime by the remarks following Proposition 1.1. In this case B_r^0 is irreducible (see Corollary 3.7) and the argument given in Section 2.1 shows that $\Phi_2(r, H) = \{1\}$.

4. Computations with cohomology groups

Let A be an abelian group and H be a finite group acting on A (determining a homomorphism of H into $\mathrm{Aut}(A)$). Let K be the corresponding semidirect product. The specified action of H on A defines A as a $\mathbb{Z}H$-module.

Recall that, with this action of $\mathbb{Z}H$ on the module A, the zeroth cohomology group $H^0(H, A)$ is the subgroup of A consisting of the fixed points of H (in other words, the centralizer of H in A). The first cohomology group $H^1(H, A)$ is in bijective correspondence with the set of K-conjugacy classes of complements of A in K, and $H^1(H, A) = 0$ if and only if all complements of A are conjugate in K (see, for example, [8, Chapter 17, Proposition 33]). Similarly, the second cohomology group $H^2(H, A)$ determines the number of extensions of A by H under this action, and $H^2(H, A) = 0$ if and only if every extension of A by H with the given action splits (see, [8, Chapter 17, Theorem 36]).

In the present section we shall be interested in computing certain cohomology groups related to our problem. For convenience we list some standard results from cohomology theory (see, for example, [8, Section 17.2]).

Lemma 4.1. *Let H be a finite group and V be a $\mathbb{Z}H$-module.*

(a) *If $V = V_1 \oplus V_2$ is a direct sum of $\mathbb{Z}H$-modules, then $H^i(H, V) = H^i(H, V_1) \oplus H^i(H, V_2)$.*

(b) (*Shapiro's lemma*) *Let K be a subgroup of H. Consider the module $V \otimes_{\mathbb{Z}K} \mathbb{Z}H$ obtained by inducing V up to H. Then $H^i(H, V \otimes_{\mathbb{Z}K} \mathbb{Z}H) \cong H^i(K, V)$.*
(c) *Let $h = |H|$. If $hV = V$, then $H^i(H, V) = 0$ for all $i \geqslant 0$.*
(d) *If H acts trivially on V, then $H^1(H, V) = \mathrm{Hom}(H, V)$.*
(e) *Suppose that $0 \to U \to V \to W \to 0$ is an exact sequence of $\mathbb{Z}H$-modules. Then we have an exact sequence*

$$0 \to H^0(H, U) \to H^0(H, V) \to H^0(H, W) \to H^1(H, U) \to H^1(H, V)$$
$$\to H^1(H, W) \to H^2(H, U) \to H^2(H, V) \to H^2(H, W) \to \cdots.$$

Remark. In particular, we shall use (b) (Shapiro's lemma) in the following situation. Suppose that hypothesis (H) holds and consider $\mathbb{Z}_k := \mathbb{Z}/k\mathbb{Z}$ as an $\mathbb{Z}H_1$-module with the trivial action. Then the induced $\mathbb{Z}H$-module is isomorphic to $D(k)$ with the conjugation action of H. Hence $H^i(H, D(k)) \cong H^i(H_1, \mathbb{Z}_k)$.

Theorem 4.2 (see [17]). *Let $H = SL(n, q)$ where $q = p^a$ for a prime p, and put $M := X(i_1, \ldots, i_a)$. Then $H^1(H, M) = 0$ unless one of the following holds*:

(i) *$a \geqslant 2$ and $M = Fr^j X((n-1)(p-1) - 1, 1, 0, \ldots, 0)$ or $Fr^j X(p, n(p-1) - 1, 0, \ldots, 0)$ for some j.*
(ii) *$a \geqslant 1$, $p = 3$, and $(n, M) = (3, Fr^j X(3, 0, \ldots, 0))$ or $(4, Fr^j X(4, 0, \ldots, 0))$ for some j.*
(iii) *$a = 1$, $p = 2$, and $(n, M) = (3, X(1)), (3, X(2))$, or $(4, X(2))$.*

Corollary 4.3. *Suppose that $r := (q^n - 1)/(q - 1)$ is prime. Then $H^1(H, M) = 0$ for every composition factor M of $B_p \otimes \mathbb{E}$ unless $H = SL(3, 2)$ and $M = X(1)$ or $X(2)$.*

Proof. We have to show that the exceptional modules in the theorem do not occur as composition factors of $B_p \otimes \mathbb{E}$ unless $H = SL(3, 2)$.

First suppose that one of the modules in (i) occurs. As we noted in Section 3.1, the action of Fr on $X(i_1, \ldots, i_a)$ induces a cyclic permutation of the indices. Hence, by Theorem 3.3, if $Fr^j X((n-1)(p-1) - 1, 1, 0, \ldots, 0)$ is a constituent of $B_p \otimes \mathbb{E}$, then $p^j((n-1)(p-1) - 1) + p^{j+1} \equiv 0 \pmod{q-1}$. This implies that $q - 1$ divides $n(p-1)p^j$. Since $q = p^a > p$ in this case and $(n, q-1) = 1$, we have a contradiction. Thus $Fr^j X((n-1)(p-1) - 1, 1, 0, \ldots, 0)$ is not a constituent of $B_p \otimes \mathbb{E}$.

Similarly, $Fr^j X(p, n(p-1) - 1, 0, \ldots, 0)$ and $Fr^j X(3, 0, \ldots, 0)$ (for $p = 3$) cannot be constituents of $B_p \otimes \mathbb{E}$, and so the modules in case (ii) do not occur.

Finally in case (iii) the condition that r is prime eliminates the possibility that $a = 1$, $p = 2$, and $n = 4$. □

Lemma 4.4. *Suppose that hypothesis* (H) *holds. Then, for each prime $p \neq \mathrm{char}(F)$, the commutator group $[D^0(p), H]$ equals $D^0(p)$. Hence, if L is an H-invariant proper subgroup of $D^0(p)$, then $D^0(p)/L$ is not centralized by H.*

Proof. Let ω be a nontrivial pth root of 1 in F. Then using the 2-transitivity of H, we can find $x \in H$ such that x maps $u = \mathrm{diag}(\omega, \omega^{-1}, 1, \ldots, 1)$ onto $x^{-1}ux = \mathrm{diag}(1, \omega^{-1}, \omega, 1, \ldots, 1)$. Hence $ux^{-1}u^{-1}x = \mathrm{diag}(\omega, 1, \omega^{-1}, \ldots, 1)$ lies in $[D^0(p), H]$. Since the latter is H-invariant and H is 2-transitive, a simple argument now show that every element from $D^0(p)$ lies in $[D^0(p), H]$.

The second statement follows since if L is an H-invariant subgroup of $D^0(p)$ such that $D^0(p)/L$ is centralized by H, then $[D^0(p), H] \leqslant L$ and so $L = D^0(p)$ from what we have just shown. □

Proposition 4.5. *Suppose that* $(r, H) \in \Pi_3$ *and* $(p, H, r) = (3, PSL(2, 11), 11)$ *or* $(2, M_{23}, 23)$. *Let* L *be the unique proper nontrivial submodule of* B_p^0 (*see Remark following Proposition* 1.4). *Then* $H^1(H, L) = 0$.

Proof. By Lemma 4.1 and Remark which follows it we have $H^1(H, B_p) \cong H^1(H_1, \mathbb{Z}_p) = \mathrm{Hom}(H_1, \mathbb{Z}_p)$. Since $H_1 \cong A_5$ and M_{22} in the two cases, we have $H_1' = H_1$ and so $\mathrm{Hom}(H_1, \mathbb{Z}_p) = 0$. Now Proposition 1.4 and part (a) of Lemma 4.1 show that $H^1(H, B_p^0) = 0$. In each case B_p^0/L is an irreducible $\mathbb{Z}H$-module. Since the centralizer of H in B_p^0/L is a $\mathbb{Z}H$-submodule, Lemma 4.4 shows that the centralizer must be trivial. In other words, $H^0(H, B_p^0/L) = 0$. Finally, applying part (e) of Lemma 4.1 to the exact sequence

$$0 \to L \to B_p^0 \to B_p^0/L \to 0$$

gives the exact sequence $0 = H^0(H, B_p^0/L) \to H^1(H, L) \to H^1(H, B_p^0) = 0$, and so $H^1(H, L) = 0$. □

4.1. Calculation of 2*-cohomology*

Suppose that $(r, H) \in \Pi_2$ with $H = PSL(n, q)$ and A is an H-stable subgroup of D^0. Then problem (III) in the Introduction asks for a description of the groups in $\Delta(A, H)$. This is a problem in group extensions and as such is related to the second cohomology group $H^2(H, A)$ although, since we have additional conditions on $G \in \Delta(A, H)$, not all abstract extensions may give suitable G. Since $|H_1 : H_1'| = q - 1$, we know from Theorems 2.3 and 1.5 that when A is a p-subgroup, G splits over A unless either $p \mid q - 1$ or $p \mid q$.

In this section we shall eliminate one of these possibilities by showing that $H^2(H, A) = 0$ unless $p \mid q - 1$. This shows that the only cases where $\Delta(A, H)$ can contain nonsplit extensions is when $p \mid q - 1$.

We use the following notation. If L is a finite group and U is a $\mathbb{Z}L$-module, then U^L denotes the submodule consisting of the points in U fixed by L (so $U^L \cong H^0(L, U)$).

Lemma 4.6.

(a) (*See* [23, *Theorem* 11.5].) *Let* N *be a normal subgroup of a group* K *and let* A *be a* $\mathbb{Z}K$*-module. Suppose that* $H^i(N, A) = 0$ *for all* i *with* $1 \leqslant i < j$. *Then the following sequence is exact*:

$$0 \to H^j\big(K/N, A^N\big) \to H^j(K, A) \to H^j(N, A)^K \to H^{j+1}\big(K/N, A^N\big) \to H^{j+1}(K, A). \tag{4}$$

In particular, this sequence is always exact when $j = 1$.

(b) (*See* [8, *Section* 17.2].) *If* A *is a* $\mathbb{Z}_k$*-module with trivial action, then for all* $i > 0$:

$$H^i(\mathbb{Z}_k, A) = \begin{cases} a \in A \mid ka = 0 & \text{if } i \text{ is odd,} \\ A/kA & \text{if } i \text{ is even.} \end{cases}$$

(c) (*See* [24, *Lemma* 7.64].) *Suppose that* K *is a perfect group, and consider* $\mathbb{Z}_p$ *as a* $\mathbb{Z}K$*-module with trivial action. Then* $H^2(K, \mathbb{Z}_p) \neq 0$ (*that is, there exist nonsplit central extensions of* $\mathbb{Z}_p$ *by* K) *if and only if* p *divides the order of the Schur multiplier* $M(K)$ *of* K.

Lemma 4.7.

(a) *Suppose that* N *is a normal subgroup of a group* K *and* A *is a* $\mathbb{Z}K$*-module with trivial action. If* N *is perfect and* $H^2(N, A) = 0$, *then* $H^2(K/N, A) \cong H^2(K, A)$.

(b) *For each prime* p *we have* $H^2(GL(m, q), \mathbb{Z}_p) = \mathbb{Z}_{(q-1,p)}$ *except possibly in the cases* $(m, q, p) = (2, 2, 2),\ (2, 3, 2),\ (2, 4, 2),\ (2, 9, 3),\ (3, 2, 2),\ (3, 3, 3),\ (3, 4, 2)$, *or* $(4, 2, 2)$.

Proof. (a) By Lemma 4.1(d), we have $H^1(N, A) = \mathrm{Hom}(N, A)$ and so $H^1(N, A) = 0$ because N is perfect. Now by (4) with $j = 2$ we have the exact sequence

$$0 \to H^2\big(K/N, A^N\big) \to H^2(K, A) \to H^2(N, A)^K.$$

Since K acts trivially on A and $H^2(N, A) = 0$, therefore $H^2(K/N, A) \cong H^2(K, A)$.

(b) First assume that $(m, q) \neq (2, 2)$ or $(2, 3)$. Put $K := GL(m, q)$ and $N := SL(m, q)$. Then N is perfect (including the case $m = 1$) and its Schur multiplier has order h where $h = 1$ except in the following cases: $(m, q, h) = (2, 4, 2),\ (2, 9, 3),\ (3, 2, 2),\ (3, 3, 3),\ (3, 4, 16)$, and $(4, 2, 2)$ (see [26,27]). By Lemma 4.6(c), $H^2(N, \mathbb{Z}_p) = 0$ except when $p \mid h$. On the other hand, $K/N \cong \mathbb{Z}_{q-1}$. Therefore part (a) of this lemma and Lemma 4.6(b) show that, if $p \nmid h$, then $H^2(GL(n, q), \mathbb{Z}_p) = H^2(\mathbb{Z}_{q-1}, \mathbb{Z}_p) = \mathbb{Z}_{(q-1,p)}$.

This leaves the two cases where $(m, q) = (2, 2)$ or $(2, 3)$. In the former case we have $GL(2, 2) \cong S_3$ which easily implies $H^2(GL(2, 2), \mathbb{Z}_p) = 0$ $(= \mathbb{Z}_{(2-1,p)})$ for $p \neq 2$. Similarly, $GL(2, 3)$ is an extension of a normal subgroup of order 8 by S_3 and so again $H^2(GL(2, 3), \mathbb{Z}_p) = 0$ $(= \mathbb{Z}_{(3-1,p)})$ if $p \neq 2$. □

Proposition 4.8. *Suppose that* $(r, H) \in \Pi_2$ *with* $H = PSL(n, q)$. *Assume that* p *is a prime with* $p \nmid q$. *Then* $H^2(H, B_p) = \mathbb{Z}_{(q-1,p)}$ *unless* $(n, q, r, p) = (3, 3, 13, 2)$.

Proof. By Shapiro's lemma (see Lemma 4.1) and the definition of B_p, we know that $H^2(H, B_p) = H^2(H_1, \mathbb{Z}_p)$ where H_1 acts trivially on $\mathbb{Z}_p$. Since $H = SL(n, q)$ when r is prime, the structure of the point stabilizer H_1 is well-known: H_1 has a normal unipotent

subgroup N of order q^{n-1} and $H_1/N \cong GL(n-1,q)$. Since $p \nmid q$, we have $|N|\mathbb{Z}_p = \mathbb{Z}_p$, and so Lemma 4.1(c) shows that $H^1(N,\mathbb{Z}_p) = H^2(N,\mathbb{Z}_p) = 0$. Now Eq. (4) with $K = H_1$, $A = \mathbb{Z}_p$, and $j = 2$ gives the exact sequence

$$0 \to H^2\big(H_1/N, \mathbb{Z}_p^N\big) \to H^2(H_1,\mathbb{Z}_p) \to 0.$$

Since H_1 acts trivially on $\mathbb{Z}_p$, $\mathbb{Z}_p^N = \mathbb{Z}_p$ and so we have $H^2(H,B_p) \cong H^2(H_1,\mathbb{Z}_p) \cong H^2(K,\mathbb{Z}_p)$ where $K = H_1/N \cong GL(n-1,q)$. Applying Lemma 4.7(b), we conclude that $H^2(H,B_p) = \mathbb{Z}_{(q-1,p)}$ for all primes p with the seven listed possible exceptions.

Since $p \nmid q$ by assumption, none of the cases $(n-1,q,p) = (2,4,2)$, $(2,9,3)$, $(3,2,2)$, $(3,4,2)$, or $(4,2,2)$ occurs. This leaves the single possible exception: $(n-1,q,p) = (2,3,2)$ as stated. □

Theorem 4.9. *Suppose that $(r,H) \in \Pi_2$ with $H = PSL(n,q)$. If q is a power of the prime p, then $H^1(H,A) = H^2(H,A) = 0$ for every finite H-stable p-subgroup A of D^0. Thus every $G \in \Delta(A,H)$ splits over A and every pair of complements are conjugate in G.*

Proof. We have $A \leqslant D^0(p^k)$ and so every H-composition factor of A is isomorphic to an irreducible constituent of B_p^0.

We first prove that $H^1(H,A) = 0$ by induction on the number of H-composition factors of A under the hypothesis that every H-composition factor of A is isomorphic to an irreducible constituent of B_p^0. If A is an irreducible $\mathbb{F}_pH$-module, then it is a direct sum of irreducible $\mathbb{E}H$-submodules and so Lemmas 4.3 and 4.1(a) show that $H^1(H,A) = 0$ (note that every $\mathbb{E}H$-module is also a $\mathbb{Z}H$-module). Now in general, if A has more than one H-composition factor, then we can choose C as a maximal H-stable subgroup of A and apply Lemma 4.1(e) to obtain the exact sequence

$$H^1(H,C) \to H^1(H,A) \to H^1(H,A/C).$$

Since the first and last term are 0 by induction, we have $H^1(H,A) = 0$ and the induction step is proved. This shows that $H^1(H,A) = 0$ for all A such that every H-composition factor of A is isomorphic to an irreducible constituent of B_p^0.

We next prove by induction on k that $H^2(H,D^0(p^k)) = 0$ for every $k \geqslant 0$. The result is trivial for $k = 0$, so suppose $k > 0$. Then Lemma 4.1(e) and the exact sequence $0 \to D^0(p^{k-1}) \to D^0(p^k) \to B_p^0 \to 0$ show that

$$H^2\big(H,D^0\big(p^{k-1}\big)\big) \to H^2\big(H,D^0\big(p^k\big)\big) \to H^2\big(H,B_p^0\big)$$

is also exact. The last term of this sequence is 0 by Proposition 4.8 and the first term is 0 by the induction hypothesis. Thus induction shows that $H^2(H,D^0(p^k)) = 0$ as required.

Finally, consider any H-stable subgroup A. Then $A < D^0(p^k)$ for some k, and so Lemma 4.1(e) gives the exact sequence

$$H^1\big(H,D^0\big(p^k\big)/A\big) \to H^2(H,A) \to H^2\big(H,D^0\big(p^k\big)\big),$$

where the first and last terms are 0 from what we have just proved. Hence we have $H^2(H, A) = 0$. □

4.2. Proof of Theorem 1.6

Theorem 1.6 claims that when G satisfies hypothesis (H) and $d := |H_1 : H_1'|$ is relatively prime to $|A(G)|$, then G splits over $A(G)$. We already know this in the special case where $A(G)$ is the direct product of an r-subgroup and a standard subgroup (see Theorem 2.3).

We first prove the theorem when $A := A(G)$ is a basic subgroup for H. Since we always have splitting over the Sylow r-subgroup of A, it is enough to consider the case where A is basic and $(|A|, rd) = 1$. Now Theorem 1.5 shows that $A = 1$ except when:

(a) $(r, H) \in \Pi_2$ with $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$ and A is a p-group with $p \mid q$, or
(b) $(r, H) = (11, PSL(2, 11))$ or $(23, M_{23})$.

However, in case (a) we have splitting by Theorem 4.9. On the other hand, splitting can be proved for the basic subgroups in case (b) by direct computations (see Section 6.3). This proves the theorem when A is basic.

The general case now follows. Every H-stable subgroup has the form $\widetilde{A} = \tilde{\pi}_m(A)$ where A is basic and $\mathrm{char}(F) \nmid m$. The hypothesis $(|\widetilde{A}|, d) = 1$ implies that $(|A|, d) = 1$ and $(m, d) = 1$. Now $G \in \Delta(\widetilde{A}, H)$ implies that $\pi_m(G) \cong G/D^0(m)$ lies in $\Delta(A, H)$ and hence splits over $A \cong \widetilde{A}/D^0(m)$. Thus there exists $K \in \Delta(D^0(m), H)$ such that $G = \widetilde{A}K$ and $\widetilde{A} \cap K = D^0(m)$. Now K splits over $D^0(m)$ by Theorem 2.3, and this gives a splitting for G over $\widetilde{A}$.

5. The set $\Delta(1, H)$

In the present section we consider the groups in $\Delta(1, H)$ for $(r, H) \in \Pi$.

We wish to classify the groups in $\Delta(1, H)$ up to conjugacy in $GL(r, F)$ ($\sim$-equivalence) and also up to conjugacy in $\mathrm{Mon}(r, F)$ ($\approx$-equivalence). The latter classification is required in order to apply Lemma 1.7.

For each $G \in \Delta(1, H)$, the restriction of π to G defines an isomorphism of G onto H, so we can attach to G a uniquely determined representation ρ of H defined by $\pi(\rho(x)) = x$ for all $x \in H$.

Lemma 5.1. *Let $G, \widetilde{G} \in \Delta(1, H)$ with corresponding representations ρ and σ, respectively. Then*

(a) *$G \sim \widetilde{G}$ if and only if for some automorphism α of H and some $c \in GL(r, F)$ we have $\rho(x) = c^{-1}\sigma(\alpha(x))c$ for all $x \in H$.*
(b) *$G \approx \widetilde{G}$ if and only if for some automorphism α of H such that $\alpha(H_1) = H_1$ and some $c \in \mathrm{Mon}(r, F)$ we have $\rho(x) = c^{-1}\sigma(\alpha(x))c$ for all $x \in H$.*

Proof. Since $G = \operatorname{Im}\rho$ and $\widetilde{G} = \operatorname{Im}\sigma$, it is clear that the conditions are sufficient for conjugacy in both cases. We consider the necessity of these conditions.

(a) If $G = c^{-1}\widetilde{G}c$ for some $c \in GL(r, F)$, then $\alpha(x) := \pi(c\rho(x)c^{-1})$ is an automorphism of H with the required property since $\sigma \circ \pi$ is the identity on $\widetilde{G}$.

(b) Now suppose that $G = c_0^{-1}\widetilde{G}c_0$ for some $c_0 \in \operatorname{Mon}(r, F)$. Since the monomial group permutes the subspaces $Fe_1, Fe_2, \ldots, Fe_r$, there exists i such that $c_0 e_i$ is a scalar multiple of e_1. Since H is transitive, there exists $y \in H$ such that $c_1 := \rho(y)$ maps e_1 onto e_i. Then $c := c_0 c_1 \in \operatorname{Mon}(r, F)$ fixes Fe_1. Now $G = c^{-1}\widetilde{G}c$ and $c^{-1}\sigma(H_1)c = \rho(H_1)$. Thus defining the automorphism α by $\alpha(x) := \pi(c\rho(x)c^{-1})$ as in (a) we find that $\alpha(H_1) = H_1$ as required. □

Now suppose that $G \in \Delta(1, H)$ and let ρ be the corresponding representation of H. Since $\rho(H_1)$ maps Fe_1 into itself, we have homomorphism $\lambda_\rho \in \operatorname{Hom}(H_1, F^*)$ defined by $\lambda_\rho(x)e_1 := \rho(x)e_1$ for all $x \in H_1$. The representation λ_ρ^H induced from λ_ρ on H_1 up to H is equivalent to ρ (see [4, Theorem (50.2)] for the case of a general field).

This leads to the following criterion.

Lemma 5.2. *Suppose $G, \widetilde{G} \in \Delta(1, H)$ and the corresponding representations of H are ρ and σ. Then $G \approx \widetilde{G}$ if and only if there is an automorphism α of H such that $\alpha(H_1) = H_1$ and $\lambda_\rho = \lambda_\sigma \circ \alpha$.*

Proof. First suppose that $G \approx \widetilde{G}$. Then, as was shown in part (b) of the previous lemma, there exists an automorphism α of H such that $\alpha(H_1) = H_1$ and $c \in \operatorname{Mon}(r, F)$ which maps Fe_1 into itself such that $\rho(x) = c^{-1}\sigma(\alpha(x))c$ for all $x \in H$. In particular, if $x \in H_1$, then $\alpha(x) \in H_1$ and so

$$\lambda_\rho(x)e_1 = \rho(x)e_1 = c^{-1}\sigma\big(\alpha(x)\big)ce_1 = c^{-1}\lambda_\sigma\big(\alpha(x)\big)ce_1 = \lambda_\sigma\big(\alpha(x)\big)e_1.$$

Hence $\lambda_\rho(x) = \lambda_\sigma(\alpha(x))$ for all $x \in H_1$ as required.

Conversely, suppose such an automorphism α exists. We claim that there exists a monomial matrix c such that $\rho(x) = c^{-1}\sigma(\alpha(x))c$ for all $x \in H$ and so $G = c^{-1}\widetilde{G}c$. First, consider the case where α is the identity, and hence $\lambda_\rho = \lambda_\sigma$. Let $t_1, \ldots, t_r$ be a set of left coset representatives of H_1 in H with $t_i e_1 = e_i$ for each i. Since $\pi(\rho(x)) = \pi(\sigma(x)) = x$ for all $x \in H$, there exist nonzero scalars η_i and ζ_i such that $\rho(t_i)e_1 = \eta_i e_i$ and $\sigma(t_i)e_1 = \zeta_i e_i$ for each i. Let $c := \operatorname{diag}(\gamma_1, \ldots, \gamma_r)$ be a diagonal matrix whose entries we shall choose later. Now for each $x \in H$ and each i there exists j such that $xe_i = e_j$ and then $t_j^{-1}xt_i \in H_1$. Hence

$$\begin{aligned} c^{-1}\sigma(x)ce_i &= c^{-1}\sigma(t_j)\sigma\big(t_j^{-1}xt_i\big)\sigma\big(t_i^{-1}\big)\gamma_i e_i = \gamma_i\zeta_i^{-1}c^{-1}\sigma(t_j)\lambda_\sigma\big(t_j^{-1}xt_i\big)e_1 \\ &= \gamma_i\zeta_i^{-1}\zeta_j\gamma_j^{-1}\lambda_\sigma\big(t_j^{-1}xt_i\big)e_j. \end{aligned}$$

Similarly $\rho(x)e_i = \eta_i^{-1}\eta_j\lambda_\rho(t_j^{-1}xt_i)e_j$. Hence if we define $\gamma_i = \zeta_i\eta_i^{-1}$ for each i, and use the fact that $\lambda_\rho = \lambda_\sigma$, we get $\rho(x)e_i = c^{-1}\sigma(x)ce_i$ for all i and so $\rho(x) = c^{-1}\sigma(x)c$ as required.

Finally, suppose that $\lambda_\rho = \lambda_\sigma \circ \alpha$ for some automorphism α of H such that $\alpha(H_1) = H_1$. Then α can be induced by conjugation by some element $c_0 \in S$ (see [6, Theorem 4.2B]). In particular, $c_0 e_1 = e_1$. Thus $\pi(\sigma(\alpha(x))) = \alpha(x) = c_0 x c_0^{-1}$ for all $x \in H$ and so we can define a representation ϕ of H into $\mathrm{Mon}(r, F)^0$ by

$$\phi(x) := c_0^{-1}\sigma\big(\alpha(x)\big)c_0 \quad \text{for all } x \in H.$$

Note that $\pi(\phi(x)) = x$ for all $x \in H$ and, if $x \in H_1$, we have

$$\phi(x)e_1 = \sigma\big(\alpha(x)\big)e_1 = \lambda_\sigma\big(\alpha(x)\big)e_1 = \lambda_\rho(x)e_1.$$

Thus $\lambda_\phi = \lambda_\rho$, and so by the special case above there exists a diagonal matrix c_1 such that $\rho(x) = c_1^{-1}\phi(x)c_1$ for all x in H. Putting $c = c_0 c_1$, we obtain $\rho(x) = c^{-1}\sigma(\alpha(x))c$ for all x. This completes the proof. □

5.1. *Representations of $H = PSL(n, q)$*

Now consider the case where $(r, H) \in \Pi_2$ with $H = PSL(n, q)$ where $q = p^a$. In this case H_1/H_1' is a cyclic group of order $q - 1$ (by definition of Π_2, we have excluded the case $(n, q) = (3, 2)$, where the order is 2).

The permutation action of H is on lines in the underlying vector space $\mathbb{F}_q^n$ and without loss in generality we may assume that H_1 is the stabilizer of the line spanned by the vector $(1, 0, \ldots, 0)^\top$. Hence the elements of H_1 are the matrices in $SL(n, q)$ $(= PSL(n, q))$ of the form

$$\begin{bmatrix} \xi & w \\ 0 & y \end{bmatrix},$$

where $\xi \in \mathbb{F}_q^*$, w is a $1 \times (n-1)$ matrix, and $y \in GL(n-1, q)$ with $\det y = \xi^{-1}$. For each of the possible groups $SL(n, q)$ we choose one particular element $z \in H_1$ as follows. If $n = 2$, then $z = \mathrm{diag}(\zeta, \zeta^{-1})$ where ζ generates the cyclic group $\mathbb{F}_q^*$. If $n \geqslant 3$, then we choose a block diagonal matrix $z = \mathrm{diag}(\zeta, y)$ where ζ generates $\mathbb{F}_q^*$ and $y \in GL(n-1, q)$ has determinant ζ^{-1} and has no eigenvalues in $\mathbb{F}_q$. For example, the matrix y can be taken to be the companion matrix of a polynomial of the form $X^{n-1} + \beta X + (-1)^{n-1}\zeta^{-1}$ where $\beta \in \mathbb{F}_q$ is chosen so that this polynomial does not vanish for any of the $q - 1$ nonzero values from $\mathbb{F}_q$. Note that in both cases $H_1 = H_1'\langle z \rangle$.

Let Γ be the cyclic group of order a consisting of the automorphisms of H which are induced by the field automorphisms $\mathrm{Gal}(\mathbb{F}_q)$; specifically, Γ is generated by γ where $\gamma(x)$ is obtained by replacing each entry of x by its pth power. Under our hypothesis (H) we know that $H = PSL(n, q) = PGL(n, q)$. Therefore, when $n = 2$, $\mathrm{Out}(H) = \Gamma$ and, when $n > 2$, $\mathrm{Out}(H)$ is a semidirect product of Γ by a group $\langle \tau \rangle$ of order 2 where $\tau(x) := (x^{-1})^T$ is the inverse transpose (see, for example, [3]). Note that $\Gamma \cong P\Gamma L(n, q)/PGL(n, q)$.

We can now determine when two monomial representations of H of degree r are equivalent (in $GL(r, F)$).

Lemma 5.3. *Suppose that* $(r, H) \in \Pi_2$ *with* $H = PSL(n, q)$ *and assume that* $\mathrm{char}(F) \nmid q$. *Define* z *as above. Suppose that* $\lambda, \mu \in \mathrm{Hom}(H_1, F^*)$.

(a) *If* λ *is different from* 1_{H_1}, *then* λ^H *is an irreducible representation of* H. (*As is well known,* $(1_{H_1})^H$ *is always reducible.*)
(b) *The following statements are equivalent*:
  (i) λ^H *is equivalent to* μ^H;
  (ii) $\lambda(z) = \mu(z)$ (*if* $n > 2$) *or* $\lambda(z) = \mu(z)$ *or* $\mu(z)^{-1}$ (*if* $n = 2$);
  (iii) $\lambda = \mu$ (*if* $n > 2$) *or* $\lambda = \mu$ *or* μ^{-1} (*if* $n = 2$).
(c) *The representation* $\lambda^H \circ \tau$ *is equivalent to* $(\lambda^{-1})^H$.

Proof. (a) If $n > 2$ then [12, Theorem 9.1.4] shows that λ^H is irreducible for each nontrivial $\lambda \in \mathrm{Hom}(H_1, F^*)$. When $n = 2$ we know that q is a power of 2 and that $PGL(2, q) = PSL(2, q)$. Hence [12, Theorem 9.1.2] shows that λ^H is irreducible in this case too. (In both cases the proofs of these results use the fact that $\mathrm{char}(F) \nmid q$.)

(b) The equivalence is trivial if λ and μ are both 1_{H_1} so we can assume λ^H is irreducible. First, suppose that $n > 2$. In this case the choice of z ensures that z has a single fixed point and hence, by the definition of an induced representation, the traces of the matrices $\lambda^H(x)$ and $\mu^H(x)$ equal $\lambda(x)$ and $\mu(x)$, respectively. Thus (i) implies $\lambda(z) = \mathrm{trace}\,\lambda^H(z) = \mathrm{trace}\,\mu^H(z) = \mu(z)$ which is (ii). Next, since $H_1 = H_1'\langle z\rangle$ and H_1' is contained in the kernels of λ and μ, therefore $\lambda(z) = \mu(z)$ implies (iii). Finally, (iii) trivially implies (i).

Now suppose that $n = 2$. In this case z has exactly two fixed points, and again the definition of induced representation shows that the traces of $\lambda^H(z)$ and $\mu^H(z)$ are $\lambda(z) + \lambda(z)^{-1}$ and $\mu(z) + \mu(z)^{-1}$, respectively. Hence (i) implies that these two traces are equal, and that implies $\lambda(z) = \mu(z)$ or $\mu(z)^{-1}$ which is (ii). The proof that (ii) implies (iii) is the same as in the case $n > 2$. Finally, a simple matrix calculation using the rational form shows that every element in $SL(2, q)$ is conjugate to its inverse. Thus, if $\lambda = \mu$ or μ^{-1}, then $\mathrm{trace}\,\lambda^H(x) = \mathrm{trace}\,\mu^H(x) = \mathrm{trace}(\mu^{-1})^H(x)$ for all $x \in H$. Since λ^H is irreducible, this implies that λ^H is equivalent to μ^H (see, for example, [14, Theorem 1.11] for the case where $\mathrm{char}(F) > 0$). □

With the notation above we define two groups Γ_1 and Γ_2 of permutations on $\mathrm{Hom}(H_1, F^*)$ as follows. The group Γ_1 is generated by the mapping $\lambda \mapsto \lambda^p$ and Γ_2 is generated by $\lambda \mapsto \lambda^p$ and $\lambda \mapsto \lambda^{-1}$. (Note that H_1/H_1' is cyclic of order $q - 1$. Hence the order of $\mathrm{Hom}(H_1, F^*)$ divides $q - 1$ and so is relatively prime to p.)

Proposition 5.4. *Suppose that* $(r, H) \in \Pi_2$ *with* $H = PSL(n, q)$ *and* $q = p^a$. *Assume that* $\mathrm{char}(F) \neq p$.

(a) *If* $n > 2$, *then the* $\approx$*-conjugacy classes in* $\Delta(1, H)$ *are in bijective correspondence with the orbits of* $\mathrm{Hom}(H_1, F^*)$ *under* Γ_1, *and the* $\sim$*-conjugacy classes are in bijective correspondence with the orbits of* $\mathrm{Hom}(H_1, F^*)$ *under the group* Γ_2.

(b) *If $n = 2$, then the $\approx$-conjugacy classes and $\sim$-conjugacy classes in $\Delta(1, H)$ coincide and are in bijective correspondence with the orbits of* $\mathrm{Hom}(H_1, F^*)$ *under the group Γ_2.*

Proof. We are going to use Lemmas 5.2 and 5.3. Since H is 2-transitive, H_1 is maximal in H and hence its own normalizer. Thus the only inner automorphisms α of H with $\alpha(H_1) = H_1$ are those induced by elements of H_1. For these automorphisms we have $\lambda \circ \alpha = \lambda$ for the class functions $\lambda \in \mathrm{Hom}(H_1, F^*)$. Thus in applying Lemma 5.2, we can restrict ourselves to outer automorphisms.

As we noted above, if $n > 2$, then $\mathrm{Out}(H)$ is the semidirect product $\Gamma\langle\tau\rangle$. The group Γ fixes H_1 and τ maps H_1 onto the stabilizer of a hyperplane which is not conjugate to H_1 in H. Thus Lemma 5.2 shows that the $\approx$-conjugacy classes in $\Delta(1, H)$ are in bijective correspondence with the orbits of $\mathrm{Hom}(H_1, F^*)$ under the mapping $\lambda \mapsto \lambda \circ \gamma = \lambda^p$; that is, the orbits of Γ_1. This proves the first part of (a). Now the second part of (b) follows using Lemmas 5.1(a) and 5.3(c).

If $n = 2$, then $\mathrm{Out}(H) = \Gamma$ and a similar argument using Lemma 5.3(c) shows that the $\approx$-conjugacy classes in $\Delta(1, H)$ are in bijective correspondence with the orbits of Γ_1 acting on the set of sets of the form $\{\lambda, \lambda^{-1}\}$ with $\lambda \in \mathrm{Hom}(H_1, F^*)$. By Lemma 5.3(c), these orbits correspond bijectively to the orbits of Γ_2 on $\mathrm{Hom}(H_1, F^*)$. □

Corollary 5.5. *Assume that* $\mathrm{char}(F) \nmid p(q-1)$ (*in particular, this holds if* $\mathrm{char}(F) = 0$).

(a) *If $n > 2$, there are*

$$\frac{1}{a}\sum_{i=0}^{a-1}\bigl(p^i - 1, p^a - 1\bigr)$$

$\approx$-conjugacy classes in $\Delta(1, H)$. If $q = 2$, the single $\approx$-conjugacy class is also a $\sim$-conjugacy class, but when $q > 2$ there are

$$\frac{1}{2a}\sum_{i=0}^{a-1}\bigl(\bigl(p^i - 1, p^a - 1\bigr) + \bigl(p^i + 1, p^a - 1\bigr)\bigr)$$

$\sim$-conjugacy classes in $\Delta(1, H)$.

(b) *If $n = 2$, there are*

$$\frac{1}{2a}\sum_{i=0}^{a-1}\bigl(\bigl(p^i - 1, p^a - 1\bigr) + \bigl(p^i + 1, p^a - 1\bigr)\bigr)$$

$\approx$-conjugacy classes in $\Delta(1, H)$ and each of these is also a $\sim$-conjugacy class.

Proof. By the hypothesis on F, $\mathrm{Hom}(H_1, F^*)$ is cyclic of order $q - 1 = p^a - 1$. The elements in Γ_1 are the permutations $\lambda \mapsto \lambda^{p^i}$ $(i = 0, 1, \ldots, a-1)$ and the number of λ

fixed by $\lambda \mapsto \lambda^{p^i}$ is clearly $(p^i - 1, p^a - 1)$. For $q = 2$, $\Gamma_1 = \Gamma_2$, but for $q > 2$ the group Γ_2 has a additional elements, namely $\lambda \mapsto \lambda^{-p^i}$ $(i = 0, 1, \ldots, a-1)$ and the permutation $\lambda \mapsto \lambda^{-p^i}$ has $(p^i + 1, p^a - 1)$ fixed point on $\mathrm{Hom}(H_1, F^*)$. Applying the "Burnside lemma" to count orbits now yields the formulae above. □

6. Describing conjugacy classes of extensions for $(r, H) \in \Pi$

Let $(r, H) \in \Pi$. We shall describe here how to construct a complete family of representatives of the $\sim$-conjugacy classes of groups G which satisfy hypothesis (H) with $\pi(G) = H$ in terms of the basic subgroups in $\Phi(r, H)$. For the classes Π_1 and Π_3 we can list the basic subgroups completely and so obtain a complete description of the extensions G. For the class Π_2 we do not have a complete description of the basic subgroups, but we can give a partial description.

By definition of the basic subgroups, every H-stable subgroup is uniquely of the form $\widetilde{A} = \tilde{\pi}_m(A)$ with $A \in \Phi(r, H)$ and $m \geqslant 1$ not divisible by $\mathrm{char}(F)$ (see Section 1.2). Lemma 1.7 shows that if we can find a complete set of representatives for the $\approx$-conjugacy classes in $\Delta(A, H)$ for $A \in \Phi(r, H)$, then application of $\tilde{\pi}_m(A)$ gives a complete set of representatives for the $\approx$-conjugacy classes in $\Delta(\tilde{\pi}_m(A), H)$ and (for $m > 1$ and $\mathrm{char}(F) \nmid m$), these are also a set of representatives for the $\sim$-classes (Lemma 2.1). It is only for the sets $\Delta(1, H)$ and $\Delta(Z^0, H)$, that we have to distinguish between the $\approx$-classes and the $\sim$-classes. Lemma 2.1 also shows that the groups in $\Delta(A, H)$ are irreducible (and so satisfy hypothesis (H)) unless $A \leqslant Z^0$. Again we must examine the representatives in $\Delta(1, H)$ and $\Delta(Z^0, H)$ separately to distinguish those which are irreducible. Note that, if $K_1, \ldots, K_s$ is a set of representatives for the $\approx$-classes (respectively, $\sim$-classes) in $\Delta(A, H)$, then $Z^0K_1, \ldots, Z^0K_s$ is a set of representatives for the corresponding classes in $\Delta(Z^0A, H)$

In most cases the characteristic of the field does not affect the result. However, exceptions arise when $\mathrm{char}(F) = p$ and $p = r$ or cases (i) or (ii) in Proposition 1.4 occur. In these exceptional cases, $\Phi_p(r, H) = \{1\}$ because D^0 contains no nontrivial p-subgroups, and there may then be fewer basic subgroups. We shall only deal with the generic case below, and leave the modifications required for the exceptional cases to the reader.

6.1. *Extensions for* $(r, H) \in \Pi_1$

In this case $H = \mathrm{Alt}(r)$ or $\mathrm{Sym}(r)$ and $r \geqslant 7$. Theorem 1.5 shows that $\Phi(r, H) = \{1, Z^0\}$. If $H = \mathrm{Alt}(r)$, then $H_1 = H_1'$ and so Lemma 5.1 shows that H is a representative of the unique $\approx$-class (and hence unique $\sim$-class) in $\Delta(1, H)$. Theorem 2.3 shows that the groups in $\Delta(Z^0, H)$ split over Z^0, and so Z^0H represents the unique $\approx$-class in $\Delta(Z^0, H)$. Now a complete set of representatives of the $\sim$-classes of groups G satisfying hypothesis (H) with $H = \mathrm{Alt}(r)$ is given by $\tilde{\pi}_m(H)$, $\tilde{\pi}_m(Z^0H)$ as m ranges over the integers > 1 which are not divisible by $\mathrm{char}(F)$ (the groups H and Z^0H have been omitted since they are reducible).

If $H = \mathrm{Sym}(r)$, then there are two nonconjugate groups isomorphic to H in $\mathrm{Mon}(r, F)$, namely, S and $\widetilde{S} := \{\varepsilon(x)x \mid x \in S\}$ (see Section 1.3). However, of these only $\widetilde{S}$ lies in

$\mathrm{Mon}(r, F)^0$ and so again there is a single $\approx$-class in $\Delta(1, H)$. Similarly $Z^0\widetilde{S}$ represents the unique $\approx$-class in $\Delta(Z^0, H)$. A complete set of representatives of the $\sim$-classes of groups G satisfying hypothesis (H) with $H = \mathrm{Sym}(r)$ is given by $\tilde{\pi}_m(\widetilde{S})$, $\tilde{\pi}_m(Z^0\widetilde{S})$ as m ranges over the integers > 1 which are not divisible by $\mathrm{char}(F)$.

6.2. Extensions for $(r, H) \in \Pi_2$

In this case $PSL(n, q) \leqslant H \leqslant P\Gamma L(n, q)$ with $q = p^a$ and Theorem 1.5 shows that

$$\Phi(r, H) = \big\{A, Z^0A \mid A \in \Phi_p(r, H)\big\}.$$

We do not have a complete description of $\Phi_p(r, H)$, although Sections 2.1 and 3 give considerable information. In general, we have a complete description of the basic subgroups of height 1 but do not know whether there are basic subgroups of greater height. However, apart from this we have enough information to complete our description of the extensions by H.

To simplify the explanation we assume that $H = PSL(n, q)$.

Lemma 6.1. *Let $\lambda_i \in \mathrm{Hom}(H_1, F^*)$ be chosen so that $K_i := \lambda_i^H(H)$ $(i = 1, \ldots, d)$ is a set of distinct representatives for the $\approx$-conjugacy classes in $\Delta(1, H)$. If q is a power of the prime p, and A is a finite H-stable p-group, then $AK_1, \ldots, AK_d$ is a set of distinct representatives for the $\approx$-conjugacy classes in $\Delta(A, H)$.*

Proof. We first show that these groups lie in distinct classes. Indeed, suppose that $A \leqslant D^0(p^k)$, say, and choose m such that $m \equiv 1 \,(\mathrm{mod}\, q-1)$ and $m \equiv 0 \,(\mathrm{mod}\, p^k)$. If $AK_i \approx AK_j$, then $\pi_m(AK_i) \approx \pi_m(AK_j)$. But for each $x \in H$ we have $\pi_m(\lambda_i^H(x)) = (\lambda_i^m)^H(x) = \lambda_i^H(x)$ because λ_i has order dividing $q-1$. Hence $\pi_m(AK_i) = K_i$ and similarly $\pi_m(AK_j) = K_j$. Thus $AK_i \not\approx AK_j$ unless $i = j$.

We now show that for each $G \in \Delta(A, H)$ we have $G \approx AK_i$ for some i. Indeed, we know that G splits over A by Theorem 4.9, and so $G = AK$ where $K \in \Delta(1, H)$. Then, for some i and some $c \in \mathrm{Mon}(r, F)$, we have $K_i = c^{-1}Kc$. Applying π we obtain $H = \pi(c)^{-1}H\pi(c)$ and so $\pi(c)$ lies in the normalizer N of H in S. By [6, Theorem 4.2B], we know that conjugation by N induces the group of all automorphisms of H which permute the point stabilizers amongst themselves (in this case the stabilizers of lines). As we have seen before, these automorphisms form the group $P\Gamma L(n, q)$. However, we know that $P\Gamma L(n, q)$ leaves every H-stable subgroup invariant (Corollary 3.8). Since $c \in DN$ this shows that $c^{-1}AKc = c^{-1}Ac \cdot c^{-1}Kc = AK_i$ as required. □

On the other hand, if $AK_1, \ldots, AK_d$ is a set of distinct representatives for the $\approx$-conjugacy classes in $\Delta(A, H)$, then it is readily seen that $Z^0AK_1, \ldots, Z^0AK_d$ is a set of distinct representatives for the $\approx$-conjugacy classes in $\Delta(Z^0A, H)$. Thus we obtain a complete set of representatives of the extensions of basic subgroups by H. This leads as above to a complete description of a set of representatives of the form $\tilde{\pi}_m(A)$ and $\tilde{\pi}_m(Z^0A)$ for the extensions of the other H-stable subgroups. The final step is to remove any groups

K_i or Z^0K_i which are reducible, and to drop some K_i or Z^0K_i when their $\sim$-classes contain more than one $\approx$-class.

6.3. Extensions for $(r, H) \in \Pi_3$

In this case $(r, H) = (7, PSL(3,2))$, $(11, PSL(2,11))$, $(11, M_{11})$, and $(23, M_{23})$. We shall deal with these one by one.

6.3.1. $(r, H) = (7, PSL(3,2))$

As Theorem 1.5 shows, $\Phi_p(7, PSL(3,2)) = \{1\}$ except for $p = 7$ and $p = 2$. Proposition 1.4 shows that B_2^0 has only one nonzero proper submodule and this has dimension 3. Corresponding to this submodule we have $A \in \Phi_2(7, PSL(3,2))$ of order 2^3 as the only basic subgroup of height 1. Computations using GAP [11] showed that there were no basic 2-subgroups of height $\geqslant 2$ and hence $\Phi_2(7, PSL(3,2)) = \{1, A\}$. We outline these computations. We can do the computations over a field of characteristic 0 (or any other characteristic $\neq 2$ or 7).

As a permutation group

$$PSL(3,2) = \big\langle (1,2,3,4,5,6,7), (2,3)(4,7) \big\rangle.$$

The split extension $D^0(2^2)H$ is constructed as a subgroup $\langle z, y, u\rangle$ of $\mathrm{Mon}(r, F)$ where the matrices z and y in S correspond to the two generators of $PSL(3,2)$ and $u := \mathrm{diag}(i, -i, 1, 1, 1, 1, 1) \in D^0(2^2)$. The subgroups of $D^0(2^2)$ which are normal in $D^0(2^2)H$ are precisely the H-stable subgroups of $D^0(2^2)$. GAP shows that $D^0(2^2)$ contains four normal subgroups which are orders 1, 2^3, 2^6, and 2^{12}, respectively, and may be identified as 1, A, $D^0(2)$, and $D^0(2^2)$. The group A consists of the cyclic transformations of $v := \mathrm{diag}(-1,-1,-1,1,1,-1,1)$ together with the identity. Since there are no basic H-stable 2-subgroups of height 2, there can be none of greater height (see Section 2.1). Thus $\Phi(7, H) = \{1, Z^0, A, Z^0A\}$.

Next we consider $\Delta(1, H)$. Since H_1/H_1' has order 2, there are two inequivalent monomial representations of degree 7. This gives rise to two $\approx$-classes (which are also $\sim$-classes) of subgroups in $\Delta(1, H)$ with representatives H and K, say, where H is reducible but K is not. We can take K as the subgroup generated by z and $\mathrm{diag}(-1,1,1,-1,1,-1,-1)y$. Now $\Delta(A, H)$ contains the split extension AH $(= AK$ in this case). Using GAP, we can find a complete set of representatives of the $\approx$-classes in $\Delta(A, H)$ as follows.

Let z, y, and v be matrices defined above. To find representatives of the $\approx$-classes in $\Delta(A, H)$ it is enough to consider the groups G in $\Delta(A, H)$ which contain z (see Lemma 2.2). Since $\pi_2(G) \in \Delta(1, H)$, we may also assume that $\pi_2(G) = H$ or K. Since the closure of $\langle v\rangle$ under conjugation by H equals A, therefore G has the form $\langle z, wy, v\rangle$ with $w \in D^0(4)$ such that $\pi_2(w) = 1$ or $\pi_2(w) = \mathrm{diag}(-1,1,1,-1,1,-1,-1)$. Indeed, it is clearly enough to restrict w to a set of coset representatives of A: in the former case we can take w ranging over the subgroup

$$C := \big\langle \mathrm{diag}(-1,-1,1,1,1,1,1), \mathrm{diag}(1,1,-1,-1,1,1,1), \mathrm{diag}(1,1,1,1,-1,-1,1) \big\rangle$$

and in the latter case w ranges over Cw_0 where $w_0 = \mathrm{diag}(i, 1, 1, i, 1, i, i)$. Using GAP, we tested these sixteen possibilities and found that only two gave groups of order $2^3 \cdot 168$. The two groups obtained were the split extension AH and the group

$$G := \langle z, \mathrm{diag}(1, 1, 1, 1, -1, -1, 1)y, v \rangle.$$

It is obvious that $\pi(G) = \pi(H) = H = \langle z, y \rangle$ and GAP verifies that both have order $2^3 \cdot |H|$. Since there is only one H-stable subgroup of order 2^3, we conclude that $A = A(G) = A(K)$. On the other hand, GAP shows that G contains an element of order 8 but AH does not. Hence G is not isomorphic to AH and so is a nonsplit extension of A (the action of the factor group on A is the same in both cases). Thus $\Delta(A, H)$ has exactly two $\approx$-classes, and AH and G are representatives of these classes.

The remaining calculations are similar to those in the previous subsections. This is the only case where we have a nonsplit extension of a basic subgroup.

6.3.2. $(r, H) = (11, PSL(2, 11))$

We know that in this case the orders of the basic subgroups are only divisible by r and 3 (see Theorem 1.5) and that there is a basic subgroup A of order 3^5 corresponding to the nonzero proper submodule of B_3^0. A calculation similar to that done for $PSL(3, 2)$ shows that in this case there is no basic 3-subgroup of height 2 and hence none of greater height. Thus $\Phi(11, PSL(2, 11)) = \{1, Z^0, A, Z^0A\}$. Since $H_1 \cong \mathrm{Alt}(5)$ is perfect, $\Delta(1, H)$ has a single $\approx$-class (which is also the only $\sim$-class) and we can take H as a representative of this class. To find representatives of the distinct $\approx$-classes in $\Delta(A, H)$ it is enough to consider the groups $G \in \Delta(A, H)$ such that $\pi_3(G) = H$. A calculation similar to that done for $PSL(3, 2)$ shows that there is only one G with this property (which is necessarily equal to AH). Thus there is a single $\approx$-class in $\Delta(A, H)$. The remaining calculations are similar to those in the preceding subsections.

6.3.3. $(r, H) = (11, M_{11})$

In this case Theorem 1.5 shows that $\Phi(11, M_{11}) = \{1, Z^0\}$. It is enough therefore to find representatives of the $\approx$-classes and $\sim$-classes in $\Delta(1, H)$. Since $H_1 \cong \mathrm{Alt}(6) \cdot 2$, there are two monomial representations of H of degree 11. The images of these representations can be taken as H and K, say, where H is reducible but K is not. Hence H and K are representatives of the two $\approx$-classes and these are also the $\sim$-classes in $\Delta(1, H)$. The remaining calculations are similar to the preceding sections.

6.3.4. $(r, H) = (23, M_{23})$

In this case Theorem 1.5 shows that the orders of the basic subgroups are only divisible by the primes r and 2 and Remark following Proposition 1.4 shows that there is one basic 2-subgroup of level 1, say A, and this group has order 2^{11}. A calculation similar to that done for $PSL(3, 2)$ now shows that H has no basic 2-subgroups of higher levels. Hence $\Phi(23, M_{23}) = \{1, Z^0, A, Z^0A\}$. Since H_1 is perfect, there is a single $\approx$-class in $\Delta(1, H)$ and we may take H as a representative. To find representatives for the $\approx$-classes in $\Delta(A, H)$ it is enough to consider the groups G such that $\pi_2(G) = H$. A calculation similar to that done for $PSL(3, 2)$ (but requiring more care since the group is much larger),

shows that there is only one such group which is necessarily the split extension AH. Thus $\Delta(A, H)$ consists of a single $\approx$-class and AH is a representative of this class. The remaining calculations are similar to those above.

Acknowledgments

The first author acknowledges partial support from NSERC Operating Grant A7171. This grant also supported a visit by the second author to Carleton University for joint work on this paper. We are grateful to V. Burichenko and A. Kleshchev for helpful comments while the paper was in preparation. In particular, Burichenko's observation (Lemma 1.7) played a crucial role in this work.

References

[1] Z. Bácskai, Finite irreducible monomial groups of prime degree, PhD thesis, Australian National University, Canberra, Australia, 1999.
[2] M. Bardoe, P. Sin, The permutation modules for $GL(n+1, F_q)$ acting on $P^n(F_q)$ and F_q^{n+1}, J. London Math. Soc. 61 (2000) 58–80.
[3] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups, Oxford Univ. Press, Oxford, 1985.
[4] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962.
[5] A.S. Detinko, Classification of irreducible maximal solvable subgroups of prime degree classical groups over finite fields, preprint, 2001.
[6] J.D. Dixon, B. Mortimer, Permutation Groups, Springer-Verlag, New York, 1996.
[7] J.D. Dixon, A. Zalesskii, Finite primitive linear groups of prime degree, J. London Math. Soc. (2) 57 (1998) 126–134.
[8] D.S. Dummit, R.M. Foote, Abstract Algebra, second ed., Prentice Hall, Englewood Cliffs, NJ, 1999.
[9] W. Feit, Some consequences of the classification of finite simple groups, in: Santa Cruz Conf. Finite Groups, California, 1979, Amer. Math. Soc., Providence, RI, 1980, pp. 175–181.
[10] D.L. Flannery, The finite irreducible monomial linear groups of degree 4, J. Algebra 218 (1999) 436–469.
[11] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.3, http://www.gap-system.org, 2002.
[12] R. Guralnick, T. Penttila, C.E. Praeger, J. Saxl, Linear groups with orders having certain large prime divisors, Proc. London Math. Soc. (3) 78 (1999) 167–214.
[13] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.
[14] B. Huppert, N. Blackburn, Finite Groups II, Springer-Verlag, Berlin, 1980.
[15] S. Jennings, The structure of the group ring of a p-group over a modular field, Trans. Amer. Math. Soc. 50 (1941) 175–185.
[16] M. Klemm, Über die Reduction von Permutation Moduln, Math. Z. 143 (1975) 113–117.
[17] A.S. Kleschev, Über die Reduktion von Permutationsmoduln, Mat. Zametki 51 (5) (1992) 43–53 (in Russian).
[18] A.S. Kondratiev, A. Zalesski, Linear groups of degree $\leqslant 27$ over residue rings, J. Algebra 240 (2001) 120–142.
[19] T.I. Kopylova, Finite irreducible solvable groups of matrices of prime degree, Vesti Akad. Navuk Belorussian SSR (ser. Fiz.–Mat. Navuk) (5) (1976) 14–22 (in Russian).
[20] V. Landazuri, G. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra 32 (1974) 418–443.

[21] B. Mortimer, The modular permutation representations of the known doubly transitive groups, Proc. London Math. Soc. (3) 41 (1980) 1–20.
[22] M. Muzychuk, The structure of submodules of the permutation module $(GL(p), V_n(p),\ p \geqslant 3)$, in: Group Representation Theory, Internat. Workshop, Haifa, 1994, p. 5, abstracts.
[23] J.J. Rotman, An Introduction to Homological Algebra, Academic Press, New York, 1979.
[24] J.J. Rotman, An Introduction to the Theory of Groups, fourth ed., Springer-Verlag, New York, 1995.
[25] M.W. Short, The Primitive Soluble Permutation Groups of Degree Less Than 256, in: Lecture Notes in Math., vol. 1519, Springer-Verlag, Berlin, 1992.
[26] R. Steinberg, Representation of algebraic groups, Nagoya Math. J. 22 (1963) 33–54.
[27] R. Steinberg, Lectures on Chevalley Groups, Yale Univ. Press, New Haven, CT, 1967.
[28] D.A. Suprunenko, Minimal irreducible solvable linear groups of prime degree, Trudy Mosk. Mat. Ob-va 29 (1973) 223–234 (in Russian).
[29] D.A. Suprunenko, Matrix Groups, in: Transl. Math. Monogr., vol. 45, Amer. Math. Soc., Providence, RI, 1976.
[30] I.D. Suprunenko, A.E. Zalesskii, Truncated symmetric powers of the natural realizations of the groups $SL_m(P)$ and $Sp_m(P)$ and their restrictions on subgroups, Siber. Mat. Zh. 31 (4) (1990) 33–46 (in Russian); Siberian Math. J. 31 (4) (1990) 555–566.
[31] I.D. Suprunenko, A.E. Zalesskii, Permutation representations and a fragment of the decomposition matrix of the symplectic and the special linear groups over a finite field, Siber. Mat. Zh. 31 (5) (1990) 46–60 (in Russian); Siberian Math. J. 31 (5) (1990) 744–755.